

高等学校网络空间安全专业规划教材

网络安全习题详解

沈鑫剡 等 编著

高等学校网络空间安全专业规划教材

网络安全习题详解

沈鑫剡　李兴德　俞海英　伍红兵　编著

清华大学出版社
北　京

内 容 简 介

本书是《网络安全》教材的配套教辅，与主教材的每一章内容相对应，提供了例题解析、选择题分析和名词解释三部分内容。

本书通过大量习题的解析过程，帮助读者加深理解网络安全中存在的大量术语及概念的本质含义和相互之间的区别，弄清、弄透网络安全理论及技术和协议的基本原理和工作过程。

本书在设计习题时，参考了全国计算机等级考试三级信息安全技术和信息安全工程师技术水平考试中的典型题型，因此，本书对参加全国计算机等级考试三级信息安全技术和信息安全工程师技术水平考试的读者而言，也是一本非常有价值的参考书。

图书在版编目（CIP）数据

网络安全习题详解/沈鑫剡等编著. —北京：清华大学出版社，2018
（高等学校网络空间安全专业规划教材）
ISBN 978-7-302-49626-7

Ⅰ. ①网…　Ⅱ. ①沈…　Ⅲ. ①计算机网络－网络安全－高等学校－题解　Ⅳ. ①TP393.08-44

中国版本图书馆 CIP 数据核字（2018）第 031775 号

责任编辑： 袁勤勇
封面设计： 傅瑞学
责任校对： 时翠兰
责任印制： 李红英

出版发行： 清华大学出版社
网　　址： http://www.tup.com.cn，http://www.wqbook.com
地　　址： 北京清华大学学研大厦 A 座　　**邮　　编：** 100084
社 总 机： 010-62770175　　**邮　　购：** 010-62786544
投稿与读者服务： 010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈： 010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载： http://www.tup.com.cn，010-62795954
印 装 者： 北京泽宇印刷有限公司
经　　销： 全国新华书店
开　　本： 185mm×260mm　　**印　张：** 12.5　　**字　　数：** 289 千字
版　　次： 2018 年 5 月第 1 版　　**印　　次：** 2018 年 5 月第1 次印刷
印　　数： 1～1500
定　　价： 35.00 元

产品编号：069873-01



前言

习题解析是学习过程中的重要一环。网络安全学科中存在大量术语和概念,有些概念之间的区别比较模糊,需要通过习题解析加深理解这些概念的本质含义和相互之间的区别。网络安全基础理论、网络安全协议、网络安全技术和计算机安全技术及其在构建安全网络方面的应用都是十分抽象的,同样需要通过习题解析分解、剖析这些内容和应用过程。因此,编写了作为教材《网络安全》配套教辅的《网络安全习题详解》。本教辅针对教材中每一章的内容,提供了例题解析、选择题分析和名词解释三部分内容。

本书在设计习题时,参考了全国计算机等级考试三级信息安全技术和信息安全工程师技术水平考试中的典型题型,因此,本书对参加全国计算机等级考试三级信息安全技术和信息安全工程师技术水平考试的读者而言,也是一本非常有价值的参考书。

限于作者的水平,本书中的错误和不足之处在所难免,殷切希望各位读者批评指正。作者 E-mail 地址为 shenxinshan@163.com。

作　者

2018 年 2 月


目 录

第1章 概 述

1.1 例题解析

【例题 1.1】 借助使用借记卡通过自动柜员机取钱的例子，说明保密性、完整性和可用性的要求。

【解析】 在取钱和账户存储过程中，必须保证密码的保密性、账户的完整性及账户存储和处理系统的可用性，而自动柜员机自身的可用性并不是十分重要。

【例题 1.2】 简述 IATF 与 P2DR 之间的联系和区别。

【解析】 P2DR 模型表明，保障信息系统安全的要素是策略、防护、检测和响应。这些要素之间的关系如下：在安全策略的控制和指导下，在综合运用防护工具的同时，利用检测工具了解和评估信息系统的安全状态，通过适当的反应将信息系统调整到最安全和风险最低的状态。但 P2DR 模型一是没有清楚地描述网络环境下的信息系统的组成、结构和行为；二是没有清楚地描述信息系统的组成、结构和行为与安全保障机制之间的相互关系；三是没有突出人员的因素，但无论是安全信息系统的实施过程，还是安全信息系统的运行和维护过程，人员都是最重要的因素；四是没有突出安全信息系统的运行过程。运行过程是人员、系统和管理的有机集成，是相互作用的过程。

IATF 是描述信息系统安全保障的指导性文件。信息系统安全保障是通过分析信息系统的风险，制订并执行相应的安全保障策略，从技术、管理、工程和人员等方面提出安全保障的要求，确保信息系统的保密性、完整性和可用性，将安全风险控制在可接受的程度的一个动态过程。与 P2DR 相比，其有以下几点不同：一是 IATF 突出了人员的因素，表明了人员在设计、实施、维护、管理和运行过程中的重要作用；二是 IATF 给出了网络环境下信息系统的组成，根据功能将其分为四个部分；三是 IATF 针对每一个组成部分给出相应的安全技术；四是 IATF 采取纵深防御战略；五是 IATF 强调了运行中的安全功能实现过程；六是 IATF 强调基于信息系统全寿命保障安全目标。

1.2 选择题分析

(1) 关于信息安全的地位和作用，以下哪一项描述是错误的？（　　）

A. 信息安全是网络时代国家生存和民族振兴的根本保障

B. 信息安全是信息社会健康发展和信息革命成功的关键因素

C. 信息安全是网络时代人类生存和文明发展的基本条件

D. 信息安全无法影响人们的工作和生活

答案：D

【分析】 信息安全已经与人们的工作和生活息息相关。

(2) 以下哪一项不是加密用于表示信息的数据的原因？(　　)

A. 防止通过获取数据还原出数据表示的信息

B. 防止通过毁坏数据毁坏数据表示的信息

C. 防止通过篡改数据篡改数据表示的信息

D. 防止因为遗失数据导致数据表示的信息泄露

答案：B

【分析】 通过毁坏数据毁坏数据表示的信息的行为不是通过数据加密可以预防的。

(3) 以下哪一项不是采用密码机的因素？(　　)

A. 加密算法越复杂，加密运算量越大，密文越不容易破译

B. 密钥长度越大，加密运算量越大，密文越不容易破译

C. 加密和解密过程要求具有实时性

D. 不允许人接触加密算法和密钥

答案：D

【分析】 密码机加密时使用的加密算法和密钥与解密时使用的解密算法和密钥都需要人为设置。

(4) 以下哪一个阶段不属于信息安全发展阶段？(　　)

A. 有线通信和无线通信阶段　　B. 计算机存储信息阶段

C. 网络阶段　　D. 云计算阶段

答案：D

【分析】 云计算是网络阶段的一种应用方式，不是单独的信息安全发展阶段。

(5) 对于有线通信和无线通信阶段，以下哪一项是使加密变得更加重要的原因？(　　)

A. 数据转换成信号后进行传播，监听经过信道传播的信号比较容易

B. 两地之间的数据传输时间变短

C. 两地之间的数据传输过程变得容易

D. 允许传输数据的两地之间的距离变得更长

答案：A

【分析】 由于敌方容易监听到经过信道传播的信号，因此，敌方很容易还原出信号表示的数据。如果不对数据加密，则敌方很容易从数据中还原出数据表示的信息。

(6) 以下哪一项不是单机状态下的安全措施？(　　)

A. 物理保护计算机，不允许非授权人员接触计算机

B. 访问控制，非授权人员无法读取或复制计算机中的信息

C. 防止计算机感染病毒

D. 禁止接入任何输出设备

答案：D

【分析】 在单机状态下，如果禁止接入任何输出设备，则将无法对该计算机进行正常

的读取或复制操作。

(7) 以下哪一项不是单机状态和网络状态之间的区别？(　　)

A. 数据转换成信号后通过链路进行传播

B. 转发节点中存储的数据

C. 可以远程实现对计算机中数据的非法访问

D. 计算机中存储、处理数据

答案：D

【分析】 计算机中存储、处理数据是单机状态下也存在的事实。

(8) 以下哪一项不是信息安全目标？(　　)

A. 保密性　　B. 完整性　　C. 可用性　　D. 及时性

答案：D

【分析】 信息安全是指保障信息系统已经存在的信息的安全。及时性是指及时更新信息系统中的信息，不属于安全范畴。

(9) 数据完整性指的是(　　)。

A. 保护网络中各系统之间交换的数据不被泄露

B. 完成两端实体的身份鉴别过程

C. 防止非法实体对用户的主动攻击，保证数据接收方接收到的信息与发送方发送的信息完全一致

D. 确保数据是由合法实体发送的

答案：C

【分析】 数据完整性的定义就是保证数据在传输过程中不被篡改和损坏。

(10) 关于网络安全目标，以下哪一项描述是错误的？(　　)

A. 可用性是指在遭受攻击的情况下，网络系统依然可以正常运转

B. 保密性是指网络中的数据不被非授权用户访问

C. 完整性是指保证不出现对已经发送或接收的信息予以否认的现象

D. 可控性是指能够限制用户对网络资源的访问

答案：C

【分析】 C选项指的是不可抵赖性的功能，不是完整性的功能。

(11) 未授权的实体得到了数据的访问权，这样做破坏了以下哪一个安全特性？(　　)

A. 机密性　　B. 完整性　　C. 合法性　　D. 可用性

答案：A

【分析】 破坏了机密性，也称为保密性。

(12) “保证数据的一致性，防止数据被非法用户篡改”指的是以下哪一个安全属性？(　　)

A. 机密性　　B. 完整性　　C. 不可否认性　　D. 可用性

答案：B

【分析】 完整性指的是信息在计算机存储和网络传输过程中，非授权用户无论何时，通过何种手段都不能删除、篡改、伪造信息。

(13) 有一种原则是对信息进行均衡、全面的防护,提高整个系统的“安全最低点”的安全性能,该原则称为(　　)。

A. 动态化原则　B. 木桶原则　C. 等级性原则　D. 整体原则

答案:B

【分析】 木桶原则是木桶的容积取决于木桶的最短板。因此,信息系统的安全取决于整个系统的“安全最低点”的安全性能。

(14) 以下哪一项不属于网络安全的范畴?(　　)

A. 网络安全基础理论　B. 网络安全协议

C. 网络安全技术　D. 网络安全意识教育

答案:D

【分析】 这里的网络安全是指与保障信息可用性、保密性、完整性、不可抵赖性和可控制性相关的理论和技术。

(15) 以下哪一项不是引发网络安全问题的因素?(　　)

A. 网络管理和使用缺陷　B. 网络技术缺陷

C. 网络信息事关重大　D. 黑客入侵

答案:D

【分析】 黑客入侵是网络安全问题,不是引发网络安全问题的因素。

(16) 以下哪一项不是引发网络安全威胁的因素?(　　)

A. 操作员安全配置不当而造成的安全漏洞

B. 在不影响网络正常工作的情况下,进行截获、窃取、破译,以获得重要机密信息

C. 安装非正版软件

D. 安装蜜罐系统

答案:D

【分析】 蜜罐系统用于诱骗黑客入侵,并监控黑客入侵过程。因此,安装蜜罐系统是安全措施。

(17) 以下哪一项不属于引发网络安全问题的原因?(　　)

A. 网络原旨是方便通信

B. 大量商务活动在网络上展开

C. 网络信息资源已经成为重要的战略资源

D. 网络安全设备发展迅速

答案:D

【分析】 网络安全设备发展迅速是增强解决网络安全问题的能力。

(18) 关于网络安全协议,以下哪一项描述是错误的?(　　)

A. 安全协议的基础是加密解密算法、报文摘要算法、鉴别机制和数字签名等

B. 安全协议用于弥补对应网络协议安全方面的缺陷

C. 安全协议用于保障对应 PDU 对等层之间的安全传输

D. 安全协议结构与 TCP/IP 体系结构无关

答案：D

【分析】 安全协议结构是基于 TCP/IP 体系结构的。

(19) 关于网络安全技术，以下哪一项描述是错误的？(　　)

A. TCP/IP 体系结构中的每一层都有对应的安全技术

B. 以太网安全技术用于防御针对以太网的攻击行为

C. 传输层安全技术可以保障互连网终端之间的安全传输过程

D. 网际层安全技术不能保障进程间的安全传输过程

答案：C

【分析】 传输层安全技术，是在网际层安全技术保障互连网终端之间的安全传输过程的基础上，保障两个进程之间的安全传输过程。

(20) 关于主机安全技术，以下哪一项描述是错误的？(　　)

A. 存在基于主机的防火墙

B. 存在基于主机的入侵检测系统

C. 存在基于主机的访问控制技术

D. 传输层和应用层安全技术只能是基于主机的安全技术

答案：D

【分析】 在 TCP/IP 体系结构中，传输层和应用层的功能只与主机有关，与路由器、交换机等互连设备无关。但有的网络安全设备，如 Web 应用防火墙，由于它的功能是保障 Web 服务器能够正常提供访问服务，因此属于应用层安全技术。

(21) TCSEC 将计算机系统安全划分为以下哪一项？(　　)

A. 三个等级七个级别　　B. 四个等级七个级别

C. 五个等级七个级别　　D. 六个等级七个级别

答案：B

【分析】 由于超 A1 级目前尚没有实施，TCSEC 实际上是将计算机系统安全划分为四类七级。

(22) 以下哪一项不是安全标准的作用？(　　)

A. 统一信息系统的安全状态和安全功能

B. 统一安全产品的安全等级和安全功能

C. 统一网络服务的安全功能和安全等级

D. 统一网络安全产品的实现技术

答案：D

【分析】 标准只能统一网络安全产品的安全等级和安全功能，不同的厂家有着各自的实现技术。

(23) 以下哪一项关于安全模型的描述是错误的？(　　)

A. 精确地描述网络环境下的信息系统的组成、结构和行为

B. 精确地描述保障信息系统安全所涉及的要素，每一个要素的作用及要素之间的相互关系

C. 精确地描述信息系统行为与保障信息系统安全所涉及的要素之间的相互

关系

D. 精确地描述各种安全保障机制的功能和实现过程

答案：D

【分析】 安全模型可以清楚地描述信息系统行为与安全保障机制之间的相互关系，不会精确地描述各种安全保障机制的功能和实现过程。

(24) 以下哪一项关于 P2DR 安全模型的描述是错误的？(　　)

A. 安全策略是核心

B. 安全保护措施的防护时间越长，信息系统越安全

C. 检测入侵和恢复系统的时间越短，信息系统越安全

D. 安全保护措施的防护时间完全取决于采用的安全技术

答案：D

【分析】 安全保护措施的防护时间既与采用的安全技术有关，也与入侵手段和入侵过程有关。

(25) 关于 P2DR 安全模型的缺陷，以下哪一项描述是错误的？(　　)

A. 没有清楚地描述网络环境下的信息系统的组成、结构和行为

B. 没有清楚地描述信息系统的组成、结构和行为与安全保障机制之间的相互关系

C. 没有突出人员的因素

D. 没有清楚地表明保障信息系统安全的过程是一个动态过程

答案：D

【分析】 P2DR 安全模型清楚地表明保障信息系统安全的过程是一个不断调整防护措施、实时检测攻击行为、并及时对攻击行为做出反应的动态过程。

(26) 关于 P2DR，以下哪一项描述是错误的？(　　)

A. 安全策略通过防护措施实施

B. 防护措施是变化的，需要动态调整

C. 检测结果是调整防护措施的依据之一

D. 响应过程可能涉及防护措施调整

答案：A

【分析】 实施安全策略是一个动态过程，检测用于了解和评估信息系统的安全状态，发现入侵行为和入侵后果，响应用于将信息系统恢复到正常状态，防护措施需要根据检测结果和响应不断调整。

(27) 关于信息保障技术框架(IATF)，以下哪一项描述是错误的？(　　)

A. IATF 核心要素由人员、技术和运行组成

B. IATF 强调基于信息系统全寿命保障安全目标

C. IATF 突出了人员在设计、实施、维护、管理和运行过程中的重要作用

D. IATF 没有清楚地描述网络环境下的信息系统的组成、结构和行为

答案：D

【分析】 IATF 给出了网络环境下信息系统的组成，根据功能将其分为四个部分。

(28) 关于审计,以下哪一项描述是正确的?(　　)

A. 保证数据接收方接收到的信息与发送方发送的信息完全一致

B. 防止因数据被截获而造成的泄露

C. 对用户和程序使用资源的情况进行记录和审查

D. 保证信息使用者都可得到相应授权的全部服务

答案:C

【分析】 审计包含两方面内容,一是通过日志记录用户和程序使用资源的情况;二是对日志进行检查、分析,以此发现用户和程序使用资源过程中可能存在的问题。

(29) 关于网络威胁对象,以下哪一项描述是正确的?(　　)

A. 网络中的信息和网络中的设备　　B. 使用网络的人员

C. 管理网络的人　　D. 转发节点和链路

答案:A

【分析】 网络环境下的信息系统由主机、链路和转发节点等网络中的设备与分布在主机、链路和转发节点中的信息组成。因此,网络中的信息和网络中的设备是网络威胁对象。

(30) 关于网络安全,以下哪一项描述是正确的?(　　)

A. 安全策略、安全技术和管理的综合

B. 安全技术实施过程

C. 根据安全策略实施安全技术

D. 强化管理

答案:A

【分析】 网络安全是策略、技术和管理的综合,单一的管理或技术都不能实现网络安全这一目标。

(31) 以下哪一项是企业安全策略的主要功能?(　　)

A. 指定用于解决特定安全问题的安全标准

B. 给出安全设备选择、配置和实施指南

C. 指定需要保护的基础设施

D. 定义必须实现的安全目标和用于实现安全目标的安全架构

答案:D

【分析】 安全策略是宏观的,更多地关注必须实现的安全目标和用于实现安全目标的安全架构,防护、检测和响应是微观的,更多地关注标准、设备和需要保护的基础设施。

(32) 计算机犯罪是指利用信息科学技术且以计算机为犯罪对象的犯罪行为,与其他类型犯罪相比具有明显的特征,下列说法中哪一项是错误的?(　　)

A. 计算机犯罪具有隐蔽性

B. 计算机犯罪具有高智能性,罪犯可能掌握一些高科技手段

C. 计算机犯罪具有很强的破坏性

D. 计算机犯罪没有犯罪现场

答案:D

【分析】 计算机犯罪是存在犯罪现场的,只是现场取证过程比较复杂和困难。

1.3 名词解释

(1) 信息安全

信息系统中的信息不会因为偶然或者恶意的原因而遭受破坏、更改和泄露,信息系统能够持续、不间断地提供信息服务。

(2) 网络安全

保障网络环境下的信息系统中分布在主机、链路和转发节点中的信息不受威胁,没有危险、危害和损失。

(3) 信息

信息是对客观世界中各种事物的运动状态和变化的反映,是客观事物之间相互联系和相互作用的表征,表现的是客观事物运动状态和变化的本质内容。

(4) 数据

记录信息的形式。

(5) 信号

数据的电气或电磁表现。

(6) 信息安全目标

保障信息的可用性、保密性、完整性、不可抵赖性和可控制性等。

(7) 安全模型

以建模的方式给出解决安全问题的方法和过程。

(8) 安全策略

为实现信息系统的安全目标,对所有与信息系统安全相关的活动所制订的规则。

(9) P2DR 安全模型

由策略(Policy)、防护(Protection)、检测(Detection)和响应(Response)这四个要素组成的安全模型。

(10) IATF

由美国国家安全局(NSA)制定的用于描述信息系统安全保障的指导性文件。

(11) 信息系统安全保障

通过分析信息系统的风险,制订并执行相应的安全保障策略,从技术、管理、工程和人员等方面提出安全保障要求,确保信息系统的保密性、完整性和可用性,将安全风险控制在可接受的程度的一个动态过程。

第2章 网络攻击

2.1 例题解析

2.1.1 简答题解析

【例题 2.1】 简述网络是病毒和蠕虫快速传播的通道的理由。

【解析】 目前常见的病毒和蠕虫的传播方式有以下几种：

① 通过移动存储媒介在主机系统之间相互复制文件；

② 浏览嵌入恶意代码的 Web 主页；

③ 打开作为邮件附件的感染病毒的宿主程序；

④ 下载并运行感染病毒的实用程序；

⑤ 在共享目录中保存感染病毒的宿主程序；

⑥ 利用主机系统漏洞上传蠕虫或感染病毒的宿主程序等。

在上述病毒传播方式中，除了通过移动存储媒介传播病毒外，其他传播方式都需通过网络进行，因此，网络是病毒和蠕虫快速传播的主要通道。

【例题 2.2】 简述恶意代码长期存在的理由。

【解析】 导致恶意代码存在的主要原因是主机系统的漏洞，包括操作系统漏洞和应用程序漏洞。在未来较长一段时间内，不可能编写出没有安全漏洞的操作系统和应用程序，因此，肯定会产生针对各种漏洞的恶意代码。网络是传播恶意代码的主要通道，网络安全技术无法完全阻隔病毒传播通路，也无法完全阻止黑客通过网络扫描到存在漏洞的主机系统，并通过网络将针对该漏洞的恶意代码上传到该主机系统并激活。

【例题 2.3】 简述黑客能够成功入侵主机系统的原因及应对策略。

【解析】 黑客能够成功入侵主机系统的原因在于以下四个方面：一是基于当前的软件设计理论和方法，从根本上消除大型软件（操作系统和大型的应用程序）的漏洞是不可能的；二是随着时间的推移，使用的用户逐渐增多，漏洞终将被发现。还有一些组织和机构专门研究流行操作系统和应用程序的漏洞，并公开研究结果；三是一旦发现漏洞，就会出现针对该漏洞的攻击软件，并流行开来；四是只要某个主机系统还没有用补丁软件修补该漏洞，黑客就可通过针对该漏洞的攻击软件对该主机系统实施攻击。

应对策略分以下三个方面。一是通过网络安全技术阻止黑客完成攻击过程。黑客成功攻击某个主机系统的步骤包括：

① 建立与该主机系统之间的传输通路；

② 通过扫描发现该主机系统的操作系统或应用程序存在漏洞且没有用补丁软件修补；

③ 使用针对该漏洞的攻击软件实施攻击。

网络安全技术可以阻止黑客完成上述步骤，如通过接入控制阻止黑客终端接入网络；通过防火墙的访问控制策略阻止黑客终端向该主机系统传输与漏洞扫描和攻击有关的报文；通过网络入侵检测系统发现黑客正在实施的扫描和攻击行为，并予以反制。

二是主机入侵检测系统能够对主机资源的访问过程实施严格管制。黑客攻击主机系统的目的或是窃取主机系统信息资源，或是破坏主机系统资源，使其崩溃，或是建立后门，以便长期控制该主机系统。完成这些操作都需黑客完成对主机系统核心资源的访问，如果主机入侵检测系统能够有效阻止黑客对主机系统核心资源的访问过程，那么黑客将无法继续对该主机系统的攻击行为。

三是及时下载并运行补丁软件。只要在黑客针对该漏洞对主机系统实施攻击前，主机系统通过补丁软件修补了该漏洞，黑客针对该漏洞对主机系统实施的攻击就无法成功。

【例题 2.4】 简述拒绝服务攻击的应对措施。

【解析】 拒绝服务攻击可以分为针对主机系统漏洞实施的拒绝服务攻击和通过过度消耗主机系统资源，使其无法与其他主机系统正常通信并提供服务的拒绝服务攻击两种，对于前一种拒绝服务攻击，如 Ping of Death、Land 等，一是可以通过修正操作系统和协议实现程序的漏洞予以解决；二是实施这种拒绝服务攻击的报文具有一定特征，网络中的信息传输设备和信息交换控制设备，如路由器、防火墙、网络入侵检测系统等，能够检测出具有该类特征的报文，并予以丢弃。

对于后一种拒绝服务攻击，如 Smurf 等，一是攻击报文通常采用原本不存在的 IP 地址，或攻击目标的 IP 地址作为源 IP 地址。二是在攻击过程中，某种类型的流量会出现异常。因此可以采用以下应对措施：可以通过交换机的接入控制过程和路由器的单播反向路径验证功能禁止源 IP 地址不正确的 IP 分组进入网络；通过分布式网络入侵检测系统对各种类型报文的流量进行监控，一旦出现较大范围的波动，立即示警并予以反制；可以通过流量管制器对一些和常见拒绝服务攻击有关的报文类型的流量进行管制。

2.1.2 设计题解析

【例题 2.5】 列出三种嗅探攻击，并简述实现机制。

【解析】 嗅探攻击一般具有以下两个特点：一是不能影响 MAC 帧源端至目的端的传输过程；二是要求攻击过程对 MAC 帧的源端和目的端是透明的。

图 2.1 展示了利用集线器实施嗅探攻击的过程，由于集线器采用广播方式转发从任何一个集线器端口接收到的 MAC 帧，因此黑客终端可以嗅探到交换机与路由器之间传输的所有 MAC 帧。

图 2.2 展示了利用 MAC 表溢出实施嗅探攻击的过程，黑客终端通过持续发送源 MAC 地址是伪造的 MAC 地址的 MAC 帧，使交换机的 MAC 表溢出，从而使交换机采用广播方式转发从任何一个交换机端口接收到的 MAC 帧，黑客终端因此可以嗅探到交换

机与路由器之间传输的所有 MAC 帧。

图 2.3 展示了利用生成树欺骗实施嗅探攻击的过程，黑客终端成为生成树的根网桥，导致终端 A 和终端 B 与终端 C 之间交换的 MAC 帧经过黑客终端。

值得强调的是，图 2.3 实际上是利用生成树欺骗实施截获攻击的过程展示。如果黑客终端复制下从一个端口接收到的 MAC 帧后，原封不动地将 MAC 帧从另一个端口转发出去，如图 2.3 所示的攻击过程对 MAC 帧的源和目的终端也是透明的。

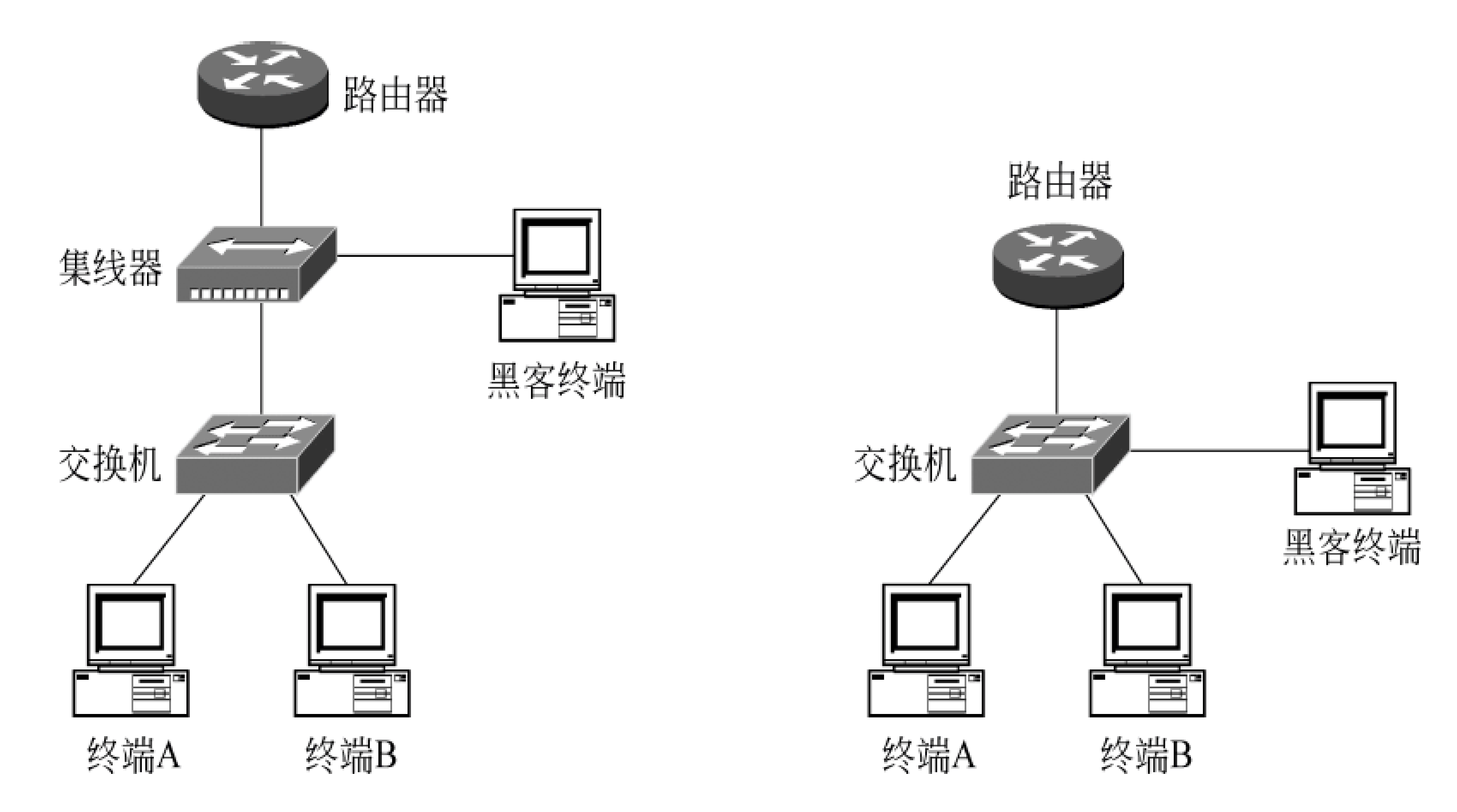


图 2.1 利用集线器实施嗅探攻击的过程 图 2.2 利用 MAC 表溢出实施嗅探攻击的过程

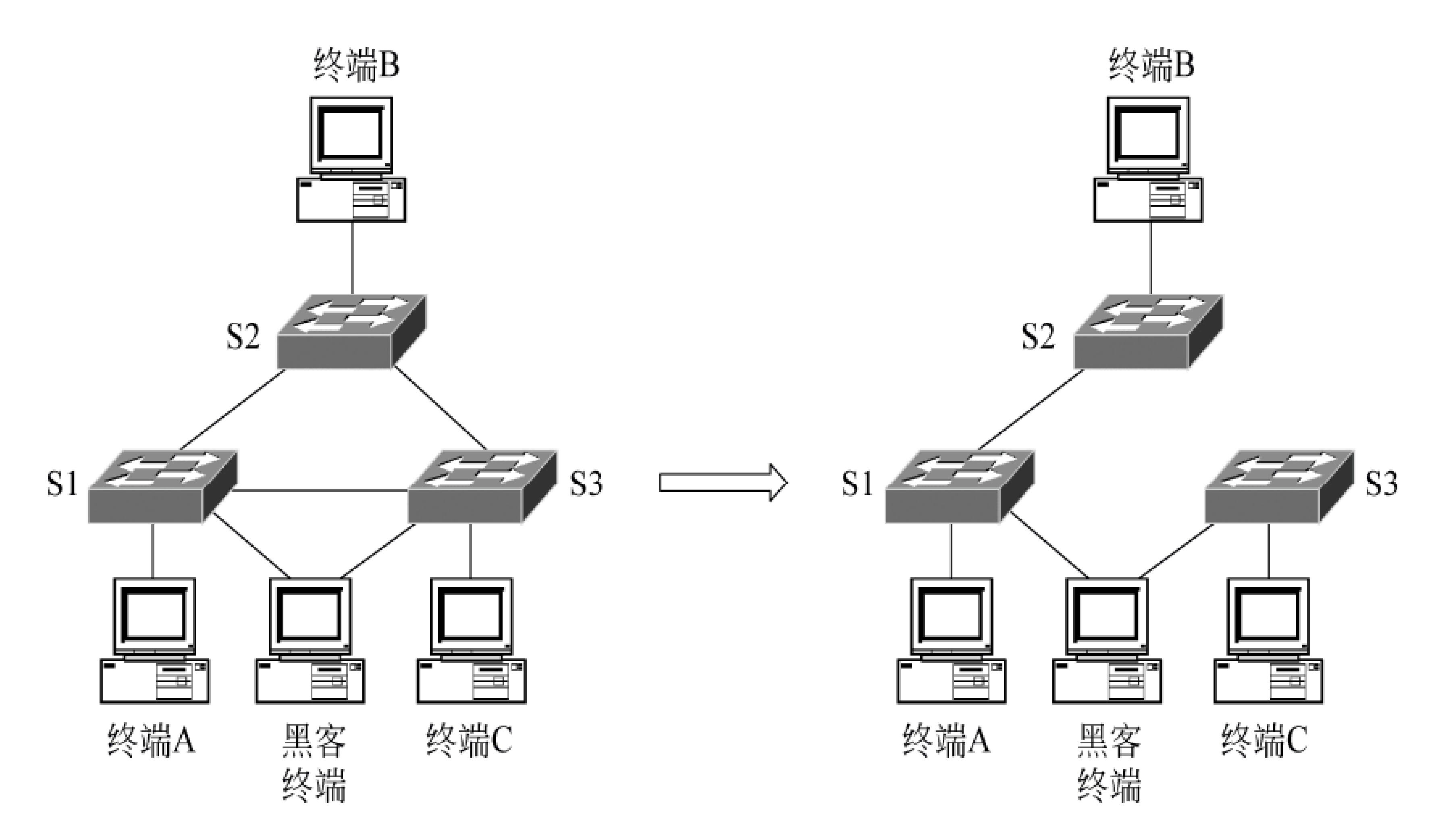


图 2.3 利用生成树欺骗实施嗅探攻击的过程

【例题 2.6】 列出三种截获攻击，并简述实现机制。

【解析】 图 2.4 展示了利用 MAC 地址欺骗实施截获攻击的过程。如果黑客终端想要截获其他终端发送给终端 C 的 MAC 帧，则黑客终端会发送一个以终端 C 的 MAC 地址为源 MAC 地址、以广播地址为目的 MAC 地址的 MAC 帧，将通往黑客终端的交换路径伪造成通往终端 C 的交换路径，使所有以终端 C 的 MAC 地址为目的 MAC 地址的 MAC 帧都被以太网错误地转发给黑客终端。

图 2.5 展示了利用 DHCP 欺骗实施截获攻击的过程。如果黑客终端想要截获其他终端发送给路由器的 IP 分组，黑客终端将一个伪造的 DHCP 服务器接入以太网，并在配

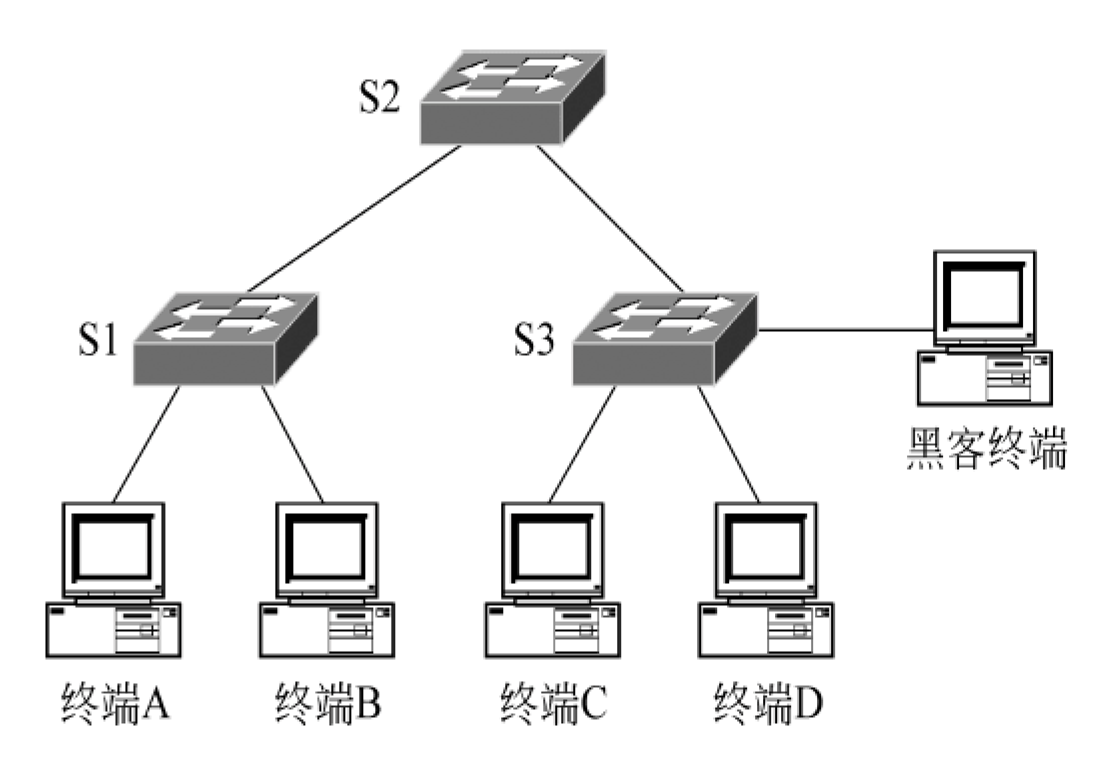


图 2.4 利用 MAC 地址欺骗实施截获攻击的过程

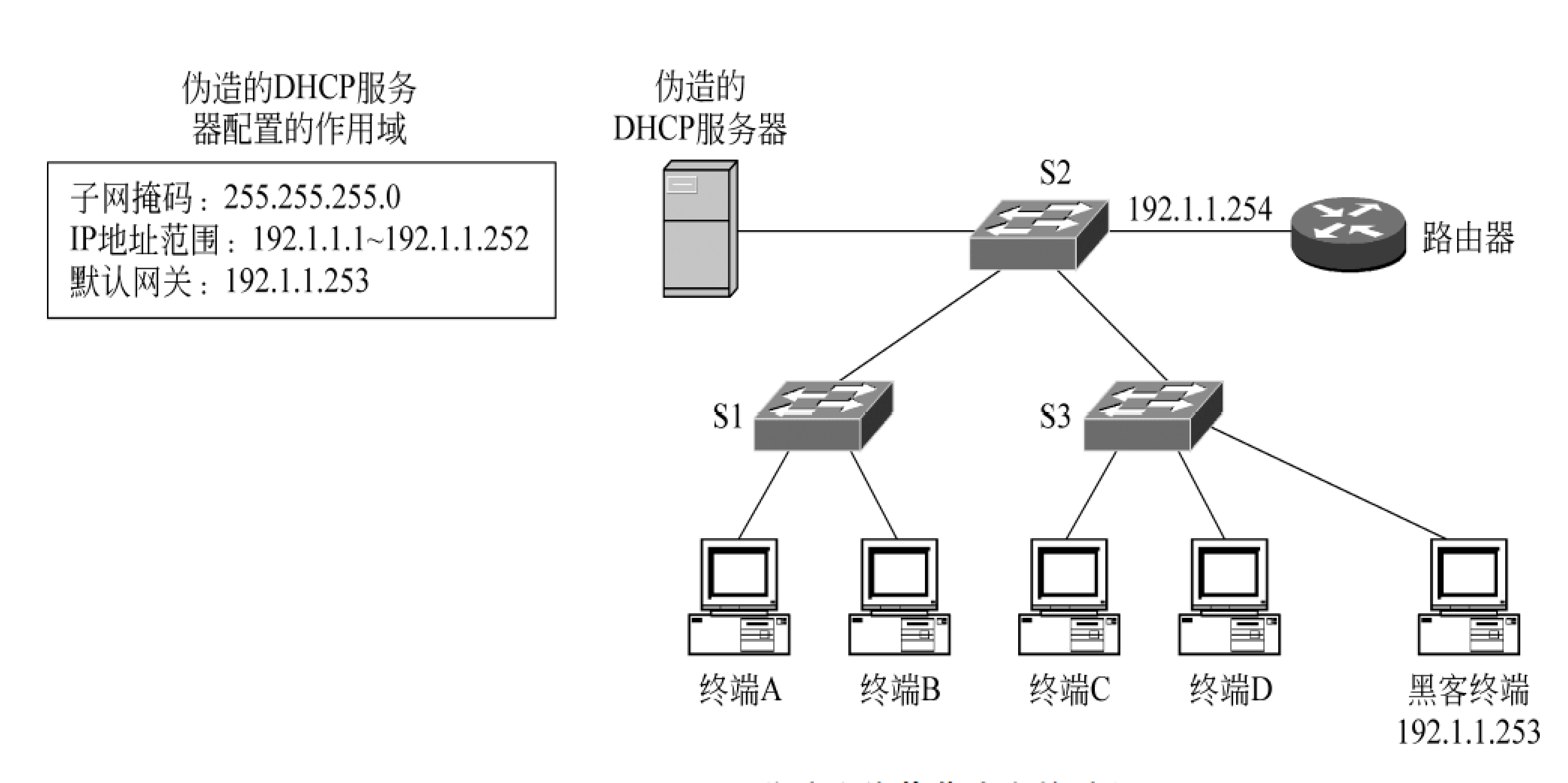


图 2.5 利用 DHCP 欺骗实施截获攻击的过程

置伪造的 DHCP 服务器的作用域时，将黑客终端的 IP 地址作为默认网关地址，使所有从伪造的 DHCP 服务器获取网络信息的终端错误地将黑客终端作为默认网关，并因此将所有发送给其他网络的 IP 分组首先发送给黑客终端。

图 2.6 展示了利用 ARP 欺骗实施截获攻击的过程。如果黑客终端想要截获其他终端发送给路由器的 IP 分组，则黑客终端会伪造一个将路由器的 IP 地址和黑客终端的

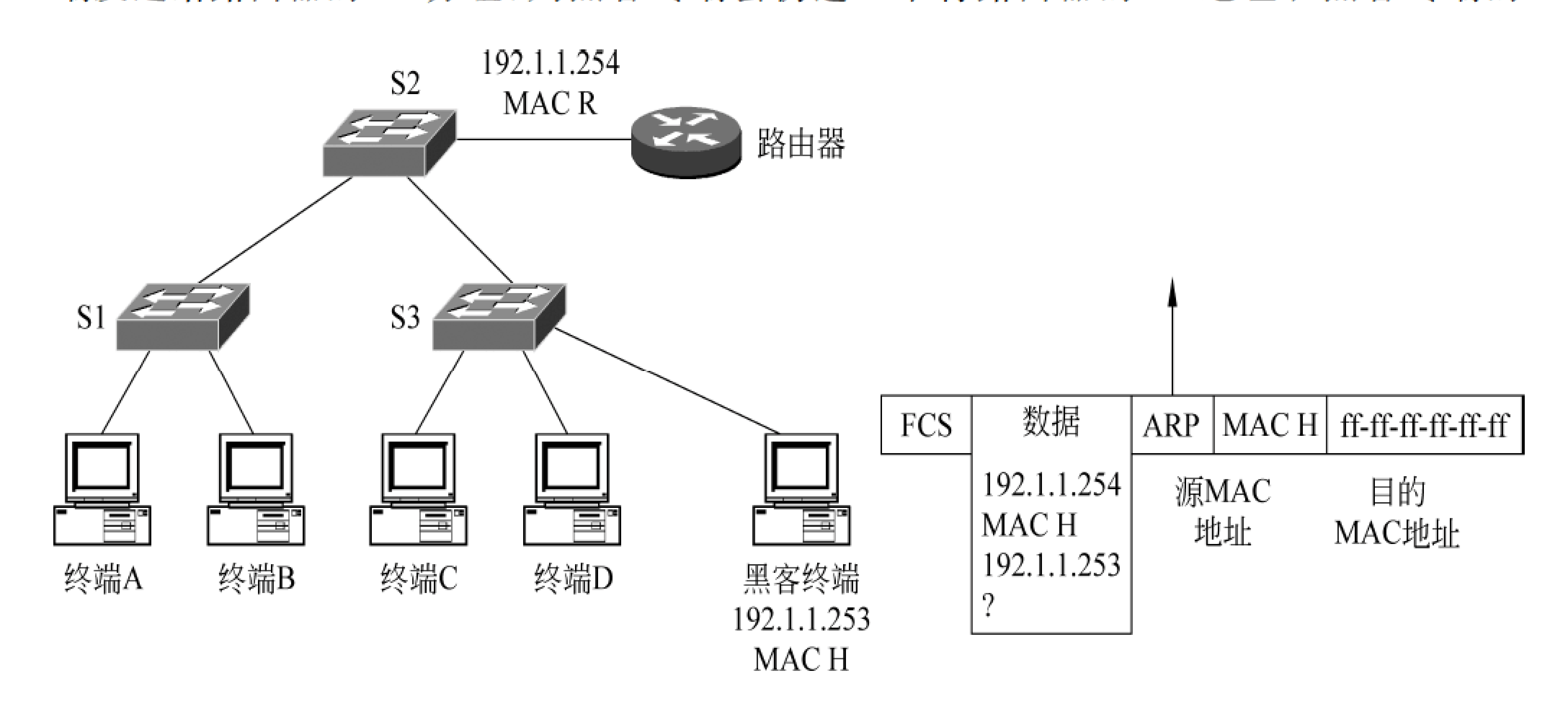


图 2.6 利用 ARP 欺骗实施截获攻击的过程

MAC地址绑定在一起的ARP报文,并在以太网中广播该ARP报文。其他终端接收到该ARP报文后,在ARP缓冲区中记录下IP地址192.1.1.254与MAC地址MAC H的绑定项。以后所有发送给默认路由器的IP分组,都被封装成以MAC H为目的MAC地址的MAC帧,该MAC帧将到达黑客终端。

【例题2.7】 互连网结构如图2.7所示,给出正常情况下路由器R2、R3和R5的路由表。如果路由器R5需要复制网络192.1.3.0/24中的终端与Web服务器之间传输的IP分组,请给出实现方法和路由器R2、R3、R5的路由表。

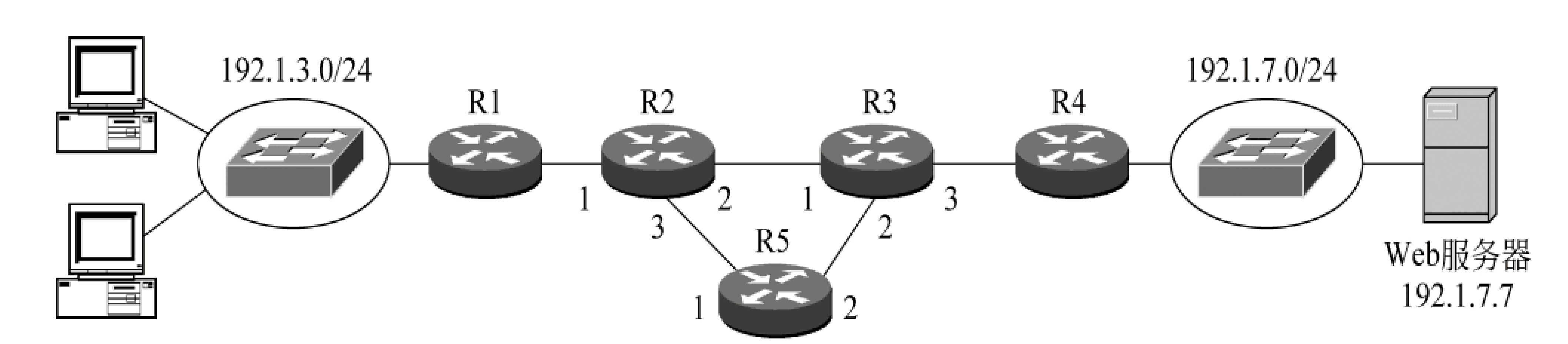


图2.7 互连网结构

【解析】 在正常情况下,路由器R2、R3和R5的路由表分别如表2.1、表2.2和表2.3所示。R2通往网络192.1.7.0/24的传输路径的下一跳是路由器R3。同样,R3通往网络192.1.3.0/24的传输路径的下一跳是路由器R2,网络192.1.3.0/24中的终端与Web服务器之间传输的IP分组不会经过路由器R5。

为了使网络192.1.3.0/24中的终端与Web服务器之间传输的IP分组经过路由器R5,路由器R5向路由器R2发送一个表明直接与网络192.1.7.0/24相连的路由项,该路由项中的距离为0,使路由器R2将用于表明通往网络192.1.7.0/24的传输路径的路由项改为表2.4所示的参数,下一跳改为路由器R5,距离改为1。路由器R5向路由器R3发送一个表明直接与网络192.1.3.0/24相连的路由项,该路由项中的距离为0,使路由器R3将用于表明通往网络192.1.3.0/24的传输路径的路由项改为表2.5所示的参数,下一跳改为路由器R5,距离改为1。因此,路由器R2将所有目的IP地址属于CIDR地址块192.1.7.0/24的IP分组转发给路由器R5,同样,路由器R3将所有目的IP地址属于CIDR地址块192.1.3.0/24的IP分组转发给路由器R5。保证网络192.1.3.0/24中的终端与Web服务器之间传输的IP分组经过路由器R5。

表2.1 路由器R2路由表

目的网络	子网掩码	输出接口	下一跳	距离
192.1.3.0	255.255.255.0	1	R1	1
192.1.7.0	255.255.255.0	2	R3	2

表2.2 路由器R3路由表

目的网络	子网掩码	输出接口	下一跳	距离
192.1.3.0	255.255.255.0	1	R2	2
192.1.7.0	255.255.255.0	3	R4	1

表 2.3　路由器 R5 路由表

目的网络	子网掩码	输出接口	下一跳	距离
192.1.3.0	255.255.255.0	1	R2	2
192.1.7.0	255.255.255.0	2	R3	2

表 2.4　路由器 R2 路由表

目的网络	子网掩码	输出接口	下一跳	距离
192.1.3.0	255.255.255.0	1	R1	1
192.1.7.0	255.255.255.0	3	R5	1

表 2.5　路由器 R3 路由表

目的网络	子网掩码	输出接口	下一跳	距离
192.1.3.0	255.255.255.0	2	R5	1
192.1.7.0	255.255.255.0	3	R4	1

【例题 2.8】 以太网结构如图 2.8 所示，如果要求黑客终端能够在其他终端不察觉的情况下，嗅探以太网中各个终端之间传输的 MAC 帧，请给出实现过程。

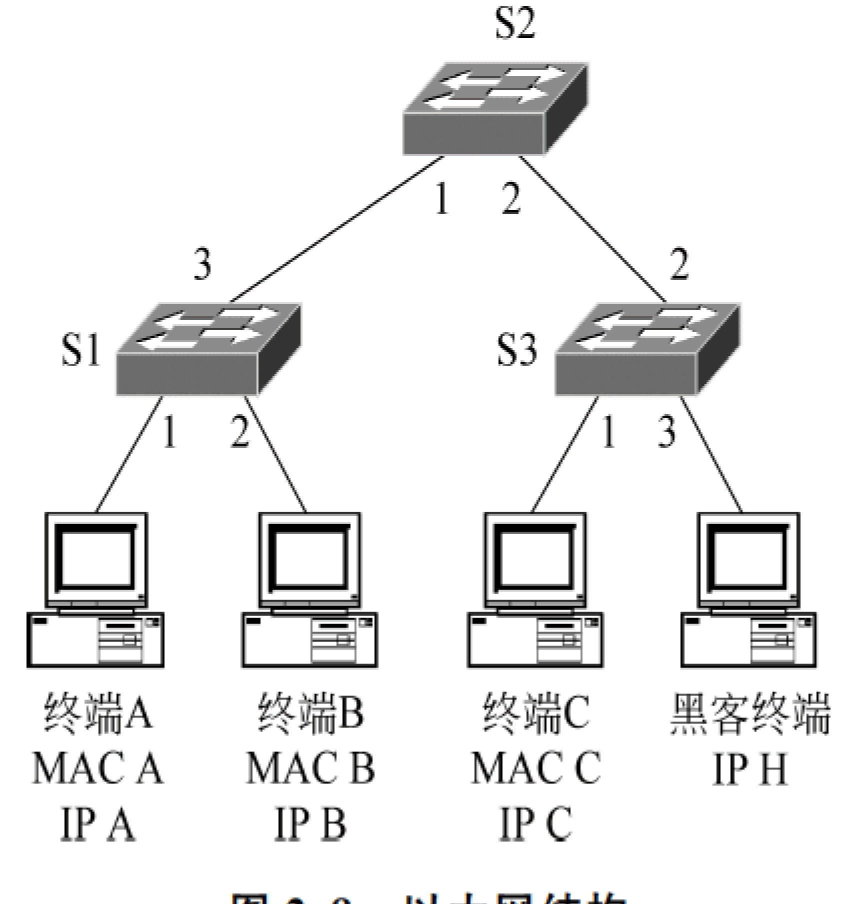


图 2.8　以太网结构

【解析】 由于该以太网结构是交换式以太网，因此，只有在各台交换机以广播方式转发各个终端之间传输的 MAC 帧时，黑客终端才能嗅探到以太网中各个终端之间传输的 MAC 帧。黑客终端需要实施 MAC 表溢出攻击，持续发送以随机产生的单播 MAC 地址为源 MAC 地址、广播地址为目的 MAC 地址的 MAC 帧。导致交换机 S1、S2 和 S3 中的 MAC 表溢出，交换机 S1、S2 和 S3 以广播方式转发各个终端之间传输的 MAC 帧。

【例题 2.9】 互连网结构如图 2.9 所示，假定由 a.com 域域名服务器完成完全合格的域名 www.a.com 的解析过程，由 b.edu 域域名服务器完成完全合格的域名 www.b.edu 的解析过程，终端 A 以 a.com 域域名服务器为本地域名服务器，终端 B 以 b.edu 域域名服务器为本地域名服务器，给出使终端 A 和终端 B 能够以完全合格的域名 www.a.com 和 www.b.edu 访问 Web 服务器 1 和 Web 服务器 2 所需的配置信息。如果黑客想要实现针对完全合格的域名 www.a.com 和 www.b.edu 的钓鱼网站，请给出实现过程和相关配置。

【解析】 在该互连网结构中，路由器 R1 连接网络 192.1.1.0/24 的接口需要配置中继地址 192.1.3.3。同样，路由器 R4 连接网络 192.1.5.0/24 的接口需要配置中继地址

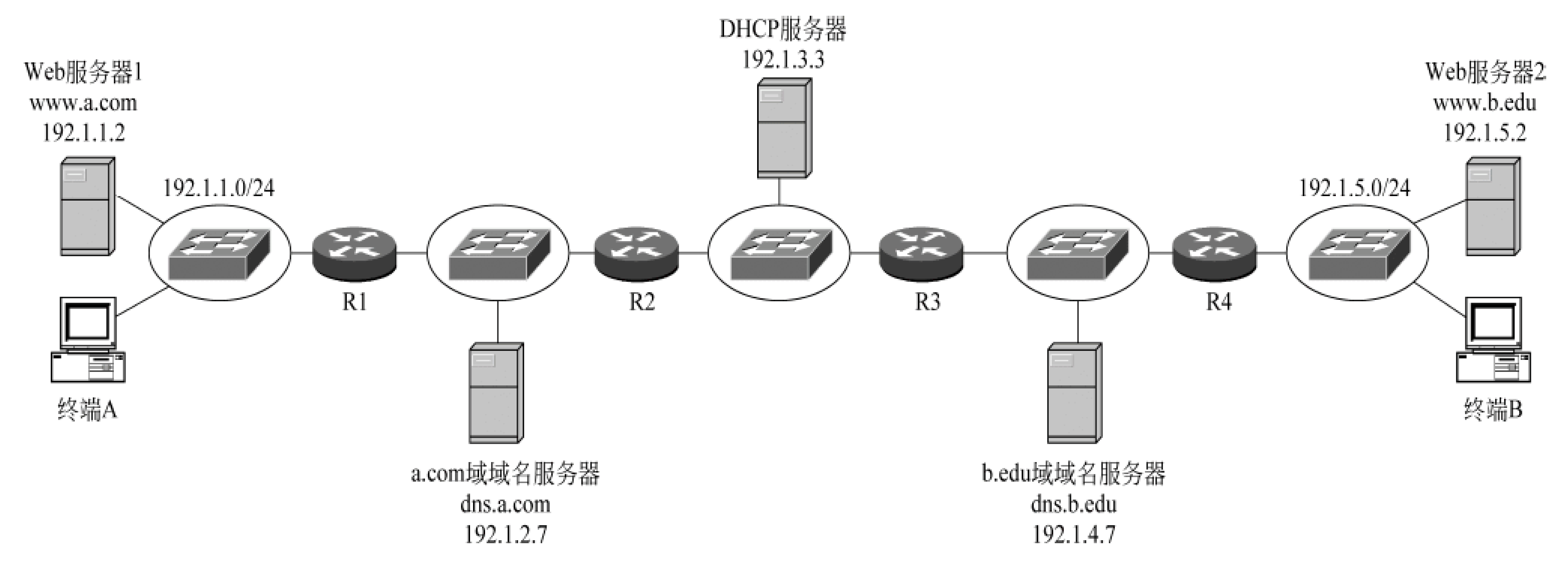


图 2.9 互连网结构

192.1.3.3，这样才能保证终端 A 和终端 B 可以通过 DHCP 服务器获取网络信息。DHCP 服务器中需要定义两个作用域，如图 2.10 所示，针对网络 192.1.1.0/24 的作用域，默认网关地址是路由器 R1 连接网络 192.1.1.0/24 的接口的 IP 地址，本地域名服务器地址是 a.com 域域名服务器的 IP 地址，IP 地址范围是属于 CIDR 地址块 192.1.1.0/24 且可以分配给终端的一组 IP 地址。针对网络 192.1.5.0/24 的作用域，默认网关地址是路由器 R4 连接网络 192.1.5.0/24 的接口的 IP 地址，本地域名服务器地址是 b.edu 域域名服务器的 IP 地址，IP 地址范围是属于 CIDR 地址块 192.1.5.0/24 且可以分配给终端的一组 IP 地址。

作用域1
默认网关地址：192.1.1.254 本地域名服务器地址：192.1.2.7 IP地址范围：192.1.1.6~192.1.1.116
作用域2
默认网关地址：192.1.5.254 本地域名服务器地址：192.1.4.7 IP地址范围：192.1.5.6~192.1.5.116

图 2.10 DHCP 服务器作用域

根据要求，由 a.com 域域名服务器完成完全合格的域名 www.a.com 的解析过程，由 b.edu 域域名服务器完成完全合格的域名 www.b.edu 的解析过程，因此，a.com 域域名服务器能够将解析完全合格的域名 www.b.edu 的解析请求转发给 b.edu 域域名服务器，同样，b.edu 域域名服务器能够将解析完全合格的域名 www.a.com 的解析请求转发给 a.com 域域名服务器。满足上述需求的 a.com 域域名服务器中的资源记录如表 2.6 所示，b.edu 域域名服务器中的资源记录如表 2.7 所示。

表 2.6 a.com 域域名服务器资源记录

名　　字	类型	值
www.a.com	A	192.1.1.2
b.edu	NS	dns.b.edu
dns.b.edu	A	192.1.4.7

表 2.7 b.edu 域域名服务器资源记录

名　　字	类型	值
www.b.edu	A	192.1.5.2
a.com	NS	dns.a.com
dns.a.com	A	192.1.2.7

实施钓鱼网站的互连网结构如图 2.11 所示，为了实施钓鱼网站，需要终端获得错误的本地域名服务器地址，因此，需要在网络中接入伪造的 DHCP 服务器，伪造的 DHCP 服务器中给出错误的本地域名服务器地址，错误的本地域名服务器地址是伪造的域名服务器的 IP 地址。两个伪造的 DHCP 服务器的作用域分别如图 2.12 所示。为了让终端

能够从伪造的 DHCP 服务器获取网络信息，直接将伪造的 DHCP 服务器接入网络 192.1.1.0/24 和网络 192.1.5.0/24 中。伪造的域名服务器中的资源记录建立完全合格的域名 www.a.com 和 www.b.edu 与两个伪造的 Web 服务器的 IP 地址之间的绑定关系，伪造的域名服务器的资源记录如表 2.8 所示。对于如图 2.11 所示的互连网结构，如果终端 A 和终端 B 从伪造的 DHCP 服务器获取网络信息，本地域名服务器地址是伪造的域名服务器的 IP 地址，当终端 A 和终端 B 需要解析完全合格的域名 www.a.com 和 www.b.edu 时，将解析请求发送给伪造的域名服务器，伪造的域名服务器返回的 IP 地址是伪造的 Web 服务器的 IP 地址。

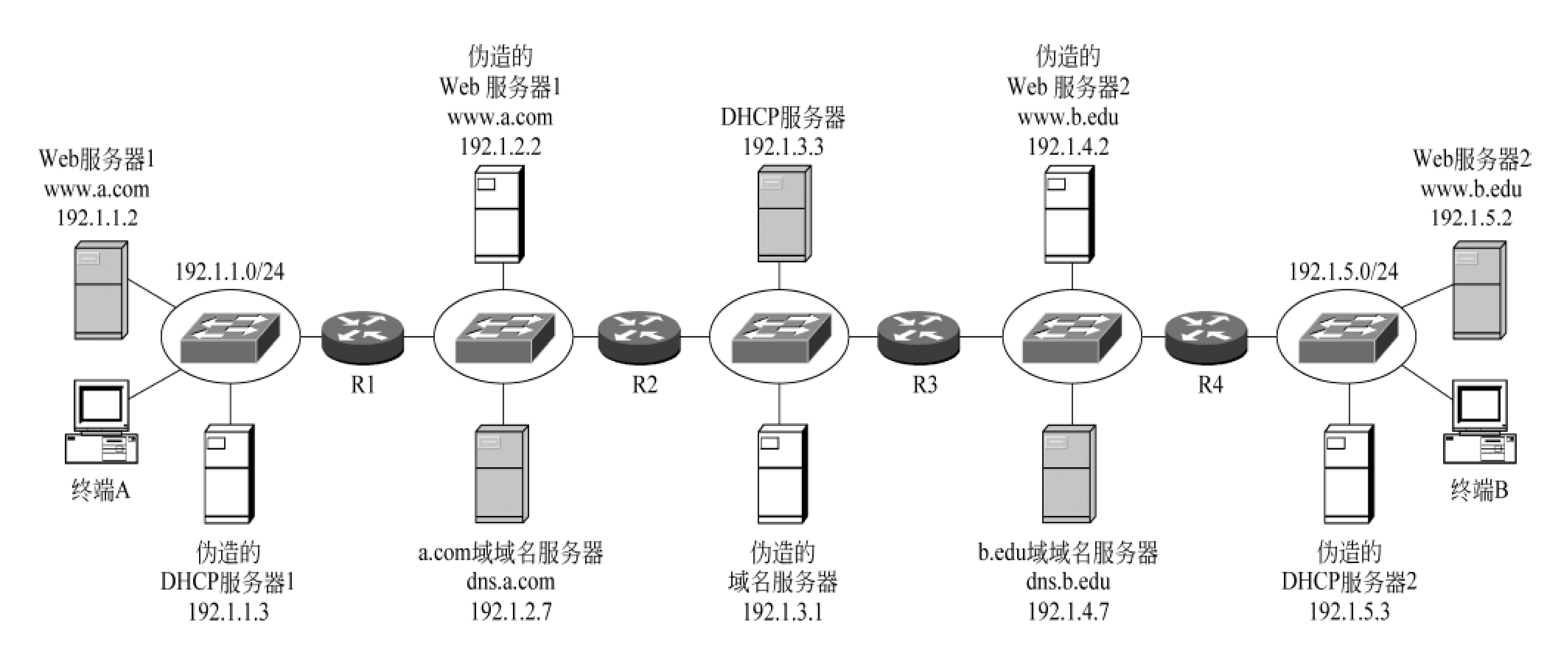


图 2.11 实施钓鱼网站的互连网结构

作用域
默认网关地址：192.1.1.254 本地域名服务器地址：192.1.3.1 IP地址范围：192.1.1.6~192.1.1.116

(a) 伪造的DHCP服务器1作用域

作用域
默认网关地址：192.1.5.254 本地域名服务器地址：192.1.3.1 IP地址范围：192.1.5.6~192.1.5.116

(b) 伪造的DHCP服务器2作用域

图 2.12 伪造的 DHCP 服务器作用域

表 2.8 伪造的域名服务器资源记录

名 字	类型	值
www.b.edu	A	192.1.4.2
www.a.com	A	192.1.2.2

2.2 选择题分析

(1) 以下哪一项关于网络攻击的描述是错误的？(　　)

A. 网络硬件、软件和协议存在漏洞

B. 网络广泛应用

C. 攻击网络有利可图

D. 所有攻击行为都会对网络和用户产生影响

答案：D

【分析】 被动攻击对于网络和用户是透明的，不会对网络和用户产生影响。

(2) 以下哪一项不属于网络面临的安全问题？(　　)

A. 病毒　　B. 拒绝服务攻击

C. 非法访问　　D. 网络设备快速更新

答案：D

【分析】 前三项都是网络目前面临的安全问题。

(3) 以下哪一项无法破坏网络的可用性？(　　)

A. 病毒　　B. 拒绝服务攻击

C. 非法访问　　D. 线缆遭受破坏

答案：C

【分析】 非法访问破坏信息的保密性，为了隐蔽，一般不会破坏信息的可用性。

(4) 以下哪一项和信息保密性无关？(　　)

A. 加密/解密算法　　B. 终端接入控制

C. 病毒　　D. 拒绝服务攻击

答案：D

【分析】 A 和 B 选项与实现信息保密性有关，C 选项与破坏信息保密性有关。拒绝服务攻击一般只与破坏信息可用性有关。

(5) 以下哪一项和信息完整性无关？(　　)

A. 加密/解密算法　　B. 报文摘要算法

C. 信息嗅探攻击　　D. 信息拦截攻击

答案：C

【分析】 A 和 B 选项与实现信息完整性有关，D 选项与破坏信息完整性有关。信息嗅探攻击一般只与破坏信息保密性有关。

(6) 以下哪一项不属于主动攻击？(　　)

A. 流量分析　　B. 重放　　C. IP 地址欺骗　　D. 拒绝服务

答案：A

【分析】 主动攻击是指会改变网络中的信息、状态和信息流模式的攻击行为。被动攻击是指不会对经过网络传输的信息、网络状态和网络信息流模式产生影响的攻击行为。流量分析只需嗅探经过网络传输的信息，因此属于被动攻击。

(7) 以下哪一项属于主动攻击？(　　)

A. 篡改和破坏数据　　B. 嗅探数据

C. 数据流分析　　D. 非法访问

答案：A

【分析】 主动攻击是指会改变网络中的信息、状态和信息流模式的攻击行为。只有 A 选项具有上述特征。

(8) 关于嗅探攻击，以下哪一项描述是错误的？(　　)

A. 嗅探攻击仅仅是复制经过网络传输的信息

B. 嗅探攻击不影响信息源端至目的端的传输过程

C. 嗅探攻击破坏信息的保密性

D. 源端或目的端可以检测到发生的嗅探攻击

答案：D

【分析】 嗅探攻击对信息的源和目的端是透明的，因此，源和目的端通常是检测不出已经发生的嗅探攻击的。

(9) 以下哪一项和信息嗅探攻击有关？(　　)

A. 操作系统漏洞　　B. 应用程序漏洞

C. 信息传输路径　　D. 主机系统的物理安保措施

答案：C

【分析】 信息嗅探攻击与信息传输路径有关。

(10) 以下哪一项和信息截获攻击有关？(　　)

A. 操作系统漏洞　　B. 应用程序漏洞

C. 配置主机系统网络信息方式　　D. 主机系统的物理安保措施

答案：C

【分析】 由伪造的 DHCP 服务器为终端配置错误的默认网关地址，使终端发送给其他网络的 IP 分组经过黑客终端，这是常见的截获攻击手段。

(11) 关于 MAC 表溢出攻击，以下哪一项描述是错误的？(　　)

A. MAC 表能够存储的转发项是有限的

B. 交换机无法鉴别 MAC 帧的源 MAC 地址和接收端口之间的绑定关系

C. 交换机广播没有转发项与之匹配的 MAC 帧

D. 不允许存在多项 MAC 地址不同但转发端口相同的转发项

答案：D

【分析】 如果某个交换机端口连接的不是终端，该交换机的转发表中可能存在多项 MAC 地址不同但转发端口是该交换机端口的转发项。黑客终端也是利用交换机允许存在多项 MAC 地址不同但转发端口相同的转发项实施 MAC 表溢出攻击的。

(12) 以下哪一项和阻止信息截获攻击无关？(　　)

A. 禁止伪造的 DHCP 服务器接入网络

B. 鉴别 DNS 资源记录

C. 鉴别路由消息

D. 用交换机取代集线器

答案：D

【分析】 实施信息截获攻击或是给出错误的通往目的终端的传输路径，或是给出错误的目的终端的 IP 地址（或物理地址），只有 D 选项与阻止这两件事情的发生无关。

(13) 以下哪一项和阻止信息嗅探攻击无关？(　　)

A. 交换机端口静态配置为全双工通信方式

B. 鉴别 DNS 资源记录

C. 交换机端口之间禁止镜像

D. 用交换机取代集线器

答案：B

【分析】 信息嗅探攻击既要窃取信息，又要不影响信息的正常传输过程，只有 B 选项与破坏这两点无关。

(14) 关于截获攻击，以下哪一项描述是错误的？（　　）

A. 截获攻击通常需要改变源和目的端之间的传输路径

B. 源和目的端之间的传输路径可以通过改变交换机转发表或路由器路由表实现

C. 截获攻击对于源和目的端是透明的

D. 截获攻击不适用于点对点物理链路两端之间的传输过程

答案：C

【分析】 截获攻击是可以被源和目的端检测到的。

(15) 以下哪一项攻击无法窃取传输过程中的数据？（　　）

A. DHCP 欺骗攻击　　B. ARP 欺骗攻击

C. 转发表溢出攻击　　D. 源 IP 地址欺骗攻击

答案：D

【分析】 A 和 B 选项能够改变数据传输路径，C 选项导致以广播方式传输数据。

(16) 关于 MAC 地址欺骗攻击，以下哪一项描述是错误的？（　　）

A. 交换机无法鉴别 MAC 帧的源 MAC 地址和接收端口之间的绑定关系

B. 交换机根据最新的 MAC 帧的源 MAC 地址和接收端口之间的绑定关系更新转发项

C. 终端可以伪造自己的 MAC 地址

D. 允许存在多项 MAC 地址相同但转发端口不同的转发项

答案：D

【分析】 在 MAC 表中，对于任何单播 MAC 地址，最多对应一项转发项。

(17) 关于 DHCP 欺骗攻击，以下哪一项描述是错误的？（　　）

A. 终端发送的 DHCP 发现消息到达所有 DHCP 服务器

B. 终端无法鉴别 DHCP 提供消息发送者的身份

C. 终端无法判别 DHCP 服务器中网络信息的正确性

D. 以太网无法阻止伪造的 DHCP 服务器提供网络信息配置服务

答案：D

【分析】 交换机可以阻止伪造的 DHCP 服务器提供网络信息配置服务。

(18) 关于 ARP 欺骗攻击，以下哪一项描述是正确的？（　　）

A. 广播的 ARP 请求报文中给出黑客终端的 MAC 地址与攻击目标的 IP 地址之间的绑定关系

B. 广播的 ARP 请求报文中给出攻击目标的 MAC 地址与黑客终端的 IP 地址之间的绑定关系

C. 广播的 ARP 请求报文中给出黑客终端的 MAC 地址与黑客终端的 IP 地址

之间的绑定关系

D. 广播的 ARP 请求报文中给出攻击目标的 MAC 地址与攻击目标的 IP 地址之间的绑定关系

答案：A

【分析】 通过给出黑客终端的 MAC 地址与攻击目标的 IP 地址之间的绑定关系，使网络中的其他节点将原本发送给攻击目标的 IP 分组错误地发送给黑客终端。

(19) 关于生成树欺骗攻击，以下哪一项描述是错误的？(　　)

A. 黑客终端有多个以太网接口

B. 黑客终端配置高优先级

C. 黑客终端发送接收 BPDU

D. 黑客终端连接交换机的链路是保证交换机之间连通性所必需的

答案：D

【分析】 删除黑客终端连接交换机的链路，不会影响网络中交换机之间的连通性。

(20) 关于路由项欺骗攻击，以下哪一项描述是错误的？(　　)

A. 接收路由消息的路由器不对路由消息进行源端鉴别和完整性检测

B. 经过黑客终端的传输路径成为路由项指明的传输路径

C. 黑客终端发送伪造的路由消息

D. 源和目的端之间所有可能的传输路径都必须经过黑客终端

答案：D

【分析】 伪造的路由消息导致错误的路由项，错误的路由项指明的源和目的端之间的传输路径才经过黑客终端。

(21) 关于 SYN 泛洪攻击，以下哪一项描述是错误的？(　　)

A. TCP 会话表中的连接项是有限的

B. 未完成建立过程的 TCP 连接占用连接项

C. 用伪造的、网络中本不存在的 IP 地址发起 TCP 连接建立过程

D. 未完成建立过程的 TCP 连接永久占用连接项

答案：D

【分析】 会话表中删除规定时间内没有完成建立过程的 TCP 连接所占用的连接项，只是这个规定时间较长，足以让黑客终端耗尽会话表中的连接项。

(22) 关于 Smurf 攻击，以下哪一项描述是错误的？(　　)

A. 封装 ICMP ECHO 请求报文的 IP 分组的源 IP 地址是攻击目标的 IP 地址

B. 封装 ICMP ECHO 请求报文的 IP 分组的目的 IP 地址是广播地址

C. 接收 ICMP ECHO 请求报文的终端回送 ICMP ECHO 响应报文

D. 单个 ICMP ECHO 请求报文只能引发单个 ICMP ECHO 响应报文

答案：D

【分析】 Smurf 攻击的特点是，黑客终端发送的单个 ICMP ECHO 请求报文可以引发多个发送给攻击目标的 ICMP ECHO 响应报文。

(23) 关于间接 DDoS 攻击，以下哪一项描述是错误的？(　　)

A. 傀儡机随机生成有效 IP 地址集

B. 正常主机系统发送对应的响应报文

C. 正常主机系统不对接收到的请求报文进行源端鉴别

D. 傀儡机发送的请求报文以随机生成的有效 IP 地址为源 IP 地址

答案：D

【分析】 傀儡机发送的请求报文以随机生成的有效 IP 地址为目的 IP 地址，以攻击目标的 IP 地址为源 IP 地址。

(24) 关于源 IP 地址欺骗攻击，以下哪一项描述是错误的？(　　)

A. 一般情况下，伪造的源 IP 地址不会对该 IP 分组的路由过程产生影响

B. 黑客终端攻击过程中不容易接收到响应报文

C. 有些信息系统将源 IP 地址作为源端身份标识符

D. 伪造的源 IP 地址不能是网络中存在的有效 IP 地址

答案：D

【分析】 在不同的攻击过程中，伪造的源 IP 地址是不同的。在 SYS 泛洪攻击过程中，伪造的 IP 地址是网络中原本不存在的 IP 地址。在 Smurf 攻击过程中，伪造的源 IP 地址是攻击目标的 IP 地址。非法登录时，伪造的源 IP 地址是具有登录权限的 IP 地址。

(25) 以下关于网络钓鱼的说法中，不正确的是(　　)。

A. 网络钓鱼融合了伪装、欺骗等多种攻击方式

B. 网络钓鱼与 Web 服务没有关系

C. 典型的网络钓鱼攻击是将被攻击者引诱到一个精心设计的钓鱼网站上

D. 网络钓鱼是“社会工程攻击”的一种形式

答案：B

【分析】 钓鱼网站通常是提供 Web 服务的服务器。

(26) 关于钓鱼网站，以下哪一项描述是错误的？(　　)

A. 黑客构建模仿某个著名网站的假网站

B. 假网站的 IP 地址与著名网站的 IP 地址相同

C. 正确的域名得到错误的解析结果

D. 用户不对访问的网站的身份进行鉴别

答案：B

【分析】 假网站的 IP 地址与著名网站的 IP 地址是不同的，但对该著名网站域名的解析结果是假网站的 IP 地址。

(27) 以下哪一项和诱骗用户登录伪造的著名网站无关？(　　)

A. 篡改 DNS 服务器的资源记录　　B. 伪造 DNS 服务器

C. 配置主机系统网络信息方式　　D. 著名网站的物理安保措施

答案：D

【分析】 诱骗用户登录伪造的著名网站需要将伪造的著名网站的 IP 地址作为著名网站域名的解析结果返回给用户。D 选项与这一过程无关。

(28) 关于非法接入无线局域网，以下哪一项描述是错误的？(　　)

A. 黑客可以通过信标帧获取 SSID
B. 黑客可以侦听到正确的一次性密钥与初始向量对
C. 黑客可以侦听到共享密钥
D. AP 通过用户提供的一次性密钥与初始向量对判别用户是否拥有共享密钥

答案：C

【分析】 黑客终端侦听不到共享密钥，也无法根据正确的一次性密钥与初始向量对推导出共享密钥。

(29) 关于非法登录，以下哪一项描述是错误的？(　　)

A. 黑客可以通过暴力破解获取授权用户的身份标识信息
B. 黑客可以通过欺骗手段获取授权用户的身份标识信息
C. 黑客可以根据授权用户的公开信息猜测出授权用户的身份标识信息
D. 黑客可以直接读取存储在介质中的用户身份标识信息

答案：D

【分析】 在存储用户身份标识信息时，一般只存储口令的单向函数运算结果，因此，无法直接从存储用户身份标识信息的介质中直接读取口令，通常也无法通过口令的单向函数运算结果还原出口令。

(30) 利用 ICMP 协议进行扫描时，以下哪一项是可以扫描的目标主机信息？(　　)

A. IP 地址　　B. 操作系统版本
C. 漏洞　　D. 弱口令

答案：A

【分析】 ICMP 可以确定配置指定 IP 地址的主机是否在线。

(31) 关于黑客入侵，以下哪一项描述是错误的？(　　)

A. 存在黑客终端与攻击目标之间的传输路径
B. 攻击目标存在漏洞
C. 黑客通过扫描发现攻击目标存在的漏洞
D. 黑客必须已经获取攻击目标的管理员账户信息

答案：D

【分析】 一般的黑客入侵有着以下两个要素：一是攻击目标是在线的，且存在漏洞；二是黑客能够利用攻击目标存在的漏洞完成入侵过程。如果黑客已经获取攻击目标的管理员账户信息，则攻击目标是否存在漏洞都不影响黑客登录。

(32) 以下哪一项和黑客远程入侵主机系统无关？(　　)

A. 操作系统漏洞　　B. 应用程序漏洞
C. 黑客和主机系统之间信息传输路径　　D. 主机系统的物理安保措施

答案：D

【分析】 主机系统的物理安保措施无法防御黑客远程入侵。

(33) 以下哪一项和病毒植入主机系统无关？(　　)

A. 操作系统漏洞　　B. 配置主机系统网络信息方式
C. 黑客和主机系统之间信息传输路径　　D. 主机系统的物理安保措施

答案：B

【分析】 A 和 C 选项是导致黑客远程入侵并上传病毒的原因，D 选项用于防止通过移动媒体直接将病毒植入主机。

(34) 以下哪一项攻击和操作系统漏洞无关？(　　)

A. 非法登录主机系统

B. 向主机系统植入病毒

C. 缓冲区溢出

D. 消耗掉主机系统连接网络的链路的带宽

答案：D

【分析】 以消耗通信系统资源为目的的拒绝服务攻击与主机系统漏洞无关。

(35) 以下哪一项表示黑客编写的旨在破坏主机系统的代码集合？(　　)

A. 恶意代码　　B. 病毒　　C. 木马　　D. 蠕虫

答案：A

【分析】 恶意代码是所有用于破坏主机系统的代码的统称。

(36) 以下哪一项表示黑客编写的旨在非法访问主机系统中信息资源的代码？(　　)

A. 恶意代码　　B. 病毒　　C. 木马　　D. 蠕虫

答案：C

【分析】 木马的主要功能就是非法访问其驻留的主机系统的信息资源。

(37) 以下哪一项表示黑客编写的、嵌入在正常程序中、具有自我复制能力的一段代码？(　　)

A. 恶意代码　　B. 病毒　　C. 木马　　D. 蠕虫

答案：B

【分析】 狭义病毒的特征有两个：一是需要宿主程序；二是具有自我复制能力。

(38) 以下哪一项表示黑客编写的、具有自动传播和自动激活特性的完整程序？(　　)

A. 恶意代码　　B. 病毒　　C. 木马　　D. 蠕虫

答案：D

【分析】 蠕虫的特征有两个：一是完整程序；二是能够在不需要人力介入的情况下，自动传播和自动激活。

(39) 以下哪一项是蠕虫能够自动传播到某个主机系统并自动激活的原因？(　　)

A. 主机系统存在漏洞

B. 主机系统下载程序

C. 主机系统收发邮件

D. 主机系统之间用移动媒介复制文件

答案：A

【分析】 蠕虫通过利用主机系统漏洞实现自动传播和自动激活。

(40) 以下哪一项操作与传播病毒无关？(　　)

A. 运行补丁软件

B. 主机系统下载程序

C. 主机系统收发邮件

D. 主机系统之间用移动媒介复制文件

答案：A

【分析】 运行补丁软件可以阻止病毒传播，其他三项操作都可以传播病毒。

(41) 以下哪一项操作不属于病毒感染？(　　)

A. 病毒将自身插入引导程序　　B. 病毒将自身插入可执行文件

C. 宏病毒将自身插入 Office 文档　　D. 建立具有管理员权限的账户

答案：D

【分析】 D 选项不属于感染病毒，而是病毒发作时实施的破坏操作。

(42) 以下哪一项不是阻止病毒传播的措施？(　　)

A. 运行补丁软件　　B. 安装查杀病毒软件

C. 禁止读/写移动存储媒介　　D. 对主机系统中重要文件加密

答案：D

【分析】 D 选项与阻止病毒传播无益，但可以减轻病毒发作时对主机系统中信息资源保密性的破坏程度。

(43) 以下哪一项不是阻止病毒经过网络传播的措施？(　　)

A. 运行补丁软件　　B. 安装查杀病毒软件

C. 禁止读/写移动存储媒介　　D. 安装主机入侵检测系统

答案：C

【分析】 经过网络传播病毒时不需要读/写移动存储媒介。

(44) 以下哪一项不是阻止病毒实施破坏操作的措施？(　　)

A. 安装主机入侵检测系统

B. 监控内部网络终端发起建立的 TCP 连接

C. 禁止读/写移动存储媒介

D. 对主机系统中重要文件加密

答案：C

【分析】 相对其他三个选项，C 选项阻止病毒实施破坏操作的作用并不明显。

(45) 以下哪一项不是恶意代码的危害？(　　)

A. 删除文件　　B. 向其他主机系统传播病毒

C. 非法访问主机系统资源　　D. 断开主机系统和网络之间的连接

答案：D

【分析】 病毒造成的危害大多需要通过网络才能完成，断开网络应该是减少危害扩散的措施。

(46) 以下哪一项不是网络成为病毒快速传播通道的原因？(　　)

A. 利用主机系统漏洞自动传播病毒

B. 通过邮件传播病毒

C. 通过 Web 页面传播病毒

D. 通过移动存储媒介在主机系统间相互复制文件传播病毒

答案：D

【分析】 该病毒传播方式与网络无关。

(47) 以下哪一项和病毒传播无关？(　　)

A. 主机系统之间复制文件　　B. 浏览 Web 主页

C. 阅读邮件　　D. 变换终端接入 Internet 的方式

答案：D

【分析】 终端用何种方式接入 Internet 与病毒传播没有太大关系。

(48) 关于狭义病毒，以下哪一项描述是错误的？(　　)

A. 嵌在宿主程序中的一段代码　　B. 具有破坏功能

C. 具有自我复制能力　　D. 能够自动激活

答案：D

【分析】 感染病毒的宿主程序一般不能自动激活，需要人工启动，或者由操作系统启动。

(49) 关于蠕虫病毒，以下哪一项描述是错误的？(　　)

A. 可以是一个独立完整程序　　B. 能够自动传播

C. 能够自动激活　　D. 只能通过利用漏洞实施传播

答案：D

【分析】 蠕虫病毒的传播方式是多种多样的，发现攻击目标漏洞，并利用漏洞实现自动传播和激活只是蠕虫病毒的传播方式之一。

(50) 关于病毒造成的危害，以下哪一项描述是错误的？(　　)

A. 病毒可以破坏主机信息的保密性

B. 病毒可以破坏主机信息的完整性

C. 病毒可以破坏主机信息的可用性

D. 病毒可以破坏主机信息的不可抵赖性

答案：D

【分析】 目前通常通过数字签名保障信息的不可抵赖性，伪造对特定信息的数字签名不是病毒可以做到的。

(51) 以下哪一项不是黑客成功实施攻击的原因？(　　)

A. 主机系统漏洞　　B. 通信协议的安全缺陷

C. 用户警惕性不够　　D. 网络分层结构

答案：D

【分析】 分层是复杂系统的有效设计方法，能够提高系统的可靠性和安全性。

(52) 以下哪一项不是黑客发现主机系统漏洞的步骤？(　　)

A. 通过主机扫描发现在线主机

B. 通过端口扫描发现开启的服务

C. 通过主动探测获得操作系统类型和版本号

D. 骗取用户口令

答案：D

【分析】 D选项和发现主机系统漏洞的过程无关。

(53) 以下哪一项是最主要的主机系统漏洞?( )

A. 缓冲区溢出 B. Unicode漏洞 C. Ping of Death D. Land

答案:A

【分析】 黑客利用缓冲区溢出漏洞,能够在管理员权限下运行自编程序,这一点对主机系统的危害极大。

(54) 以下哪一项是解决主机系统漏洞的较好办法?( )

A. 消灭主机系统漏洞

B. 不让黑客知道已经发现的主机系统漏洞

C. 网络隔绝黑客扫描主机系统的途径

D. 将存在漏洞的主机系统和网络断开

答案:C

【分析】 其他三个选项中,A和B选项做不到,D选项是笨办法。

(55) 以下哪一项不是网络中用于隔绝黑客扫描主机系统途径的机制?( )

A. 接入控制 B. 网络间信息交换控制

C. 入侵检测系统的异常检测 D. 主机系统用户登录控制

答案:D

【分析】 登录的前提是已经建立黑客和主机系统之间的传输通路。

(56) 以下哪一项不是对主机系统实施的拒绝服务攻击?( )

A. Ping of Death B. SYN泛洪

C. Smurf D. 穷举法猜测用户登录口令

答案:D

【分析】 拒绝服务攻击是使主机系统丧失服务能力,D选项不会使主机系统丧失服务能力。

(57) 以下哪一项是缓冲区溢出的最大危害?( )

A. 使系统崩溃 B. 使系统运行出错

C. 管理员权限下运行黑客程序 D. 侵占其他用户内存

答案:C

【分析】 如果在管理员权限下运行黑客程序,黑客可以任意处置系统资源。

(58) 利用以下哪一项缺陷可以实现SYN泛洪攻击?( )

A. 操作系统漏洞 B. 通信协议缺陷

C. 缓冲区溢出 D. 用户警惕性不够

答案:B

【分析】 TCP连接建立过程存在缺陷。

(59) 以下哪一项是蠕虫病毒传播的主因?( )

A. 缓冲区溢出漏洞

B. 从服务器下载文件

C. 收发电子邮件

D. 通过移动媒介在主机系统间复制文件

答案：A

【分析】 黑客利用缓冲区溢出漏洞实现在管理员权限下运行自编程序是蠕虫能够自动传播并激活的基础。

(60) 以下哪一项不是以破坏信息保密性为目的的攻击行为？(　　)

A. 信息嗅探　　B. 信息截获　　C. 安装后门程序　　D. DDoS

答案：D

【分析】 拒绝服务攻击一般以破坏可用性为目的。

(61) 以下哪一项不是以破坏信息完整性为目的的攻击行为？(　　)

A. 信息嗅探　　B. 信息截获

C. 路由项欺骗攻击　　D. ARP 欺骗攻击

答案：A

【分析】 破坏信息完整性既需要截获信息，也需要篡改信息。

(62) 以下哪一项不是以破坏信息可用性为目的的攻击行为？(　　)

A. Ping of Death　　B. SYN 泛洪

C. 安装后门程序　　D. DDoS

答案：C

【分析】 后门程序为了隐蔽，一般不会影响主机系统的正常服务功能。

(63) 以下哪一项攻击行为与主机系统漏洞无关？(　　)

A. Ping of Death　　B. Land

C. 安装后门程序　　D. Smurf

答案：D

【分析】 这种拒绝服务攻击与主机系统漏洞无关。

(64) 安装主机入侵检测系统，对以下哪一项攻击行为作用不大？(　　)

A. 窃取信息资源　　B. 篡改注册表

C. 安装后门程序　　D. Smurf

答案：D

【分析】 加强主机系统自身功能对抵御这种拒绝服务攻击作用不大。

(65) 安装网络入侵检测系统，对以下哪一项攻击行为作用不大？(　　)

A. 信息嗅探　　B. 利用缓冲区溢出运行黑客程序

C. 安装后门程序　　D. Smurf

答案：A

【分析】 网络入侵防御系统需要发现异常信息流，然后才能对异常信息流实施干预，信息嗅探攻击不会导致信息流异常。

(66) 防火墙实施的网络间信息交换控制，对以下哪一项攻击行为作用不大？(　　)

A. ARP 欺骗　　B. 木马外泄信息资源

C. Ping of Death　　D. SYN 泛洪

答案：A

【分析】 ARP 欺骗攻击在网络内部进行,无须经过防火墙。

(67) 交换机提供的安全技术,对以下哪一项攻击行为作用不大?( )

A. ARP 欺骗　　B. 源 IP 地址欺骗

C. 伪造 DHCP 服务器　　D. Ping of Death

答案:D

【分析】 需要拼装完分片后产生的所有数据片才能发现这项攻击,交换机一般不具有这项功能。

(68) 关于黑客入侵和病毒,以下哪一项描述是错误的?( )

A. 黑客和病毒结合可以使病毒快速蔓延

B. 病毒削弱主机系统安全,方便黑客入侵

C. 黑客成功入侵后,上传病毒

D. 黑客和病毒必须相互依赖,缺一不可

答案:D

【分析】 黑客和病毒结合,对网络安全构成严重威胁,但黑客入侵和病毒传播可以独立进行,例如黑客可以入侵某个存在漏洞但没有感染病毒的主机系统。

(69) 关于计算机病毒,以下哪一项描述是正确的?( )

A. 计算机病毒既不具有破坏性,也不具有传染性

B. 计算机病毒只具有破坏性,不具有传染性

C. 计算机病毒既具有破坏性,也具有传染性

D. 计算机病毒只具有传染性,不具有破坏性

答案:C

【分析】 破坏性和传染性是计算机病毒具有的两大特征。

(70) 关于病毒发展趋势,以下哪一项描述是错误的?( )

A. 病毒技术与黑客技术日益融合在一起

B. 计算机病毒制造者的主要目的只是炫耀自己高超的技术

C. 计算机病毒的数量呈指数性成长,传统的基于特征检测的防毒软件渐渐显得力不从心

D. 由于在互连网上可以下载病毒编写工具,从而使计算机病毒的编写变得越来越容易

答案:B

【分析】 目前计算机病毒制造者的主要目的是获利。

(71) 以下哪一项关于宏病毒的描述是正确的?( )

A. 宏病毒主要感染可执行文件

B. 宏病毒仅感染办公自动化程序编制的文档

C. 宏病毒主要感染软盘、硬盘的引导扇区或主引导扇区

D. CIH 病毒属于宏病毒

答案:B

【分析】 宏病毒是利用 Office 文档中的宏功能实现的,只能感染 Office 文档。

(72) 下列功能中,哪一项功能不是综合漏洞扫描包含的?( )

A. IP 地址扫描　　B. 端口号扫描

C. 恶意程序扫描　　D. 漏洞扫描

答案:C

【分析】 IP 地址扫描用于发现在线主机,端口号扫描用于发现主机打开的端口,漏洞扫描用于发现主机应用程序和操作系统存在的漏洞,但一般无法对主机进行恶意程序扫描。

(73) 关于 SYN 泛洪攻击,以下哪一项描述是错误的?( )

A. SYN 泛洪攻击利用 TCP 固有安全缺陷

B. SYN 泛洪攻击伪造原本不存在的终端发起 TCP 连接建立过程

C. SYN 泛洪攻击用于耗尽攻击目标的 TCP 会话表中的连接项

D. SYN 泛洪攻击破坏攻击目标的保密性

答案:D

【分析】 SYN 泛洪攻击破坏攻击目标的可用性,使其无法响应正常用户的建立 TCP 连接请求。

(74) 以下哪一项不是 Smurf 攻击的技术机理?( )

A. 将攻击目标的 IP 地址作为 ICMP ECHO 请求报文的源 IP 地址

B. 将 ICMP ECHO 请求报文广播给某个网络中的所有终端

C. 所有接收到 ECHO 请求报文的终端向报文的源终端回送 ECHO 响应报文

D. 广播 ICMP ECHO 请求报文浪费网络带宽和终端处理时间

答案:D

【分析】 Smurf 攻击的重点不是通过广播 ICMP ECHO 请求报文浪费网络带宽和终端处理时间,而是通过向攻击目标回送大量 ICMP ECHO 响应报文使攻击目标丧失与其他终端正常通信的能力。

(75) 以下哪一项不是 DHCP 欺骗攻击的技术机理?( )

A. 网络中可以存在多台 DHCP 服务器

B. 终端随机选择为其配置网络信息的 DHCP 服务器

C. 伪造的网络配置信息会造成终端严重的安全后果

D. 多台 DHCP 服务器可能造成终端 IP 地址重复

答案:D

【分析】 终端 IP 地址重复是多台 DHCP 服务器共存需要解决的问题,不是 DHCP 欺骗攻击的技术机理。

(76) 以下哪一项不是 ARP 欺骗攻击的技术机理?( )

A. 终端接收到 ARP 报文,记录 ARP 报文中的 IP 地址与 MAC 地址对

B. 如果 ARP 缓冲区中已经存在 IP 地址与 MAC 地址对,以该 MAC 地址作为该 IP 地址的解析结果

C. 可以在 ARP 报文中伪造 IP 地址与 MAC 地址对

D. ARP 缓冲区中的 IP 地址与 MAC 地址对存在寿命

答案：D

【分析】 ARP 缓冲区中的 IP 地址与 MAC 地址对存在寿命不是实施 ARP 欺骗攻击所需要的。

(77) 以下哪一项不是路由项欺骗攻击的技术机理？(　　)

A. 路由器选择最短路径

B. 黑客终端伪造与攻击网络直接相连的路由消息

C. 路由器将通往攻击网络的传输路径的下一跳改为黑客终端

D. 黑客终端接收其他路由器发送的路由消息

答案：D

【分析】 黑客终端是否接收其他路由器发送的路由消息与实施路由项欺骗攻击无关。

(78) 以下哪一项不是间接 DDoS 攻击的技术机理？(　　)

A. 黑客终端成功将木马程序植入多台傀儡机中

B. 黑客终端向傀儡机发送针对特定攻击目标的攻击命令

C. 每一台傀儡机随机选择正常主机系统，向正常主机系统发送 ICMP ECHO 请求报文

D. 傀儡机发送的 ICMP ECHO 请求报文以傀儡机的 IP 地址为源 IP 地址

答案：D

【分析】 傀儡机发送的 ICMP ECHO 请求报文以攻击目标的 IP 地址为源 IP 地址。

(79) 关于拒绝服务攻击，以下哪一项描述是错误的？(　　)

A. 阻塞主机连接网络的链路

B. 消耗掉主机用于提供服务的资源

C. 通过植入病毒，让主机无法正常运行

D. 通过植入病毒，复制主机中的重要信息

答案：D

【分析】 拒绝服务攻击的目的是破坏主机或网络的可用性，复制重要信息的目的是破坏主机中信息的保密性。

2.3 名词解释

(1) 网络攻击

指利用网络存在的漏洞和安全缺陷对网络中的硬件、软件及信息进行的攻击，其目的是破坏网络中信息的保密性、完整性、可用性、可控制性和不可抵赖性，削弱甚至瘫痪网络的服务功能。

(2) 被动攻击

不会对经过网络传输的信息、网络状态和网络信息流模式产生影响的攻击行为。

(3) 主动攻击

会改变网络中的信息、状态和信息流模式的攻击行为。

(4) MAC 表溢出攻击

黑客终端通过发送大量源 MAC 地址不同的 MAC 帧，使 MAC 表溢出，导致交换机广播所有以正常单播 MAC 地址为目的 MAC 地址的 MAC 帧的攻击行为。

(5) MAC 地址欺骗攻击

黑客终端通过发送源 MAC 地址为攻击目标的 MAC 地址的 MAC 帧，使交换机错误地将通往黑客终端的交换路径作为通往攻击目标的交换路径的攻击行为。

(6) DHCP 欺骗攻击

通过在网络中接入伪造的 DHCP 服务器，使终端从伪造的 DHCP 服务器获得错误的网络信息的攻击行为。

(7) ARP 欺骗攻击

通过在广播的 ARP 请求报文中给出黑客终端的 MAC 地址与攻击目标的 IP 地址之间的绑定关系，导致网络中的其他节点将原本发送给攻击目标的 IP 分组错误地发送给黑客终端的攻击行为。

(8) 生成树欺骗攻击

黑客终端通过配置高优先级，将自己作为生成树的根交换机，从而使其他终端之间传输的 MAC 帧经过黑客终端的攻击行为。

(9) 路由项欺骗攻击

黑客终端通过发送伪造的路由消息，使路由器中的路由项发生错误，导致黑客终端成为源和目的端之间传输路径必须经过的节点，源和目的端之间传输的 IP 分组全部被黑客终端截获的攻击行为。

(10) SYN 泛洪攻击

通过快速消耗掉 Web 服务器 TCP 会话表中的连接项，使正常的 TCP 连接建立过程因为会话表中连接项耗尽而无法正常进行的攻击行为。

(11) Smurf 攻击

黑客终端广播一个以攻击目标的 IP 地址为源 IP 地址的 ICMP ECHO 请求报文，导致网络中的所有终端向攻击目标发送 ICMP ECHO 响应报文，从而阻塞攻击目标连接网络的链路的攻击行为。

(12) 直接 DDoS

由已经攻陷的多个主机系统(俗称为傀儡机)直接向攻击目标发送大量无用的 IP 分组，使攻击目标丧失服务能力的攻击行为。

(13) 间接 DDoS

由已经攻陷的多个主机系统(俗称为傀儡机)向其他正常主机系统发送大量无用的 IP 分组，这些 IP 分组经过这些正常主机系统反射后，被送往攻击目标，并因此使攻击目标丧失服务能力的攻击行为。

(14) 源 IP 地址欺骗攻击

一种在实施过程中黑客终端发送的 IP 分组，不是以黑客终端真实的 IP 地址作为源 IP 地址，而是用其他终端的 IP 地址，或者伪造一个本不存在的 IP 地址作为 IP 分组的源 IP 地址的攻击行为。

(15) 钓鱼网站

黑客构建模仿某个著名网站的假网站,且能够引诱用户将访问该假网站的过程作为访问该著名网站的过程的攻击行为。

(16) 非法登录

黑客非法获取某个授权用户的身份标识信息,如用户名和口令,冒用该授权用户登录网络设备或服务器的攻击行为。

(17) 黑客入侵

黑客利用主机系统存在的漏洞,远程入侵主机系统的过程。

(18) 狭义病毒

一段嵌在宿主程序中,具有破坏功能和自我复制能力的代码。

(19) 恶意代码

黑客编写的旨在破坏主机系统的代码集合。

(20) 蠕虫

一种具备完整程序特性的恶意代码,能够自动传播到其他系统,并具有自动激发功能,因而能够快速传播。

(21) 木马

一种恶意代码,其主要功能在于削弱主机系统的安全性,并盗取主机系统的信息资源。

第3章 加 密 算 法

3.1 例 题 解 析

3.1.1 简答题解析

【例题 3.1】 简述安全加密算法的特点。

【解析】 一是加密运算过程必须足够复杂，除了通过穷举法破译密文外，没有其他更有效的破译密文的方法；二是密钥长度必须足够长，以此保证，使用普通计算机破译密文时，用穷举法破译密文所需的时间超出密文的有效期。使用高性能计算机破译密文时，破译密文付出的代价超出密文价值；三是经过广泛试验，可以证明无法通过网格计算以较小成本用穷举法破译密文。

【例题 3.2】 列出 Feistel 分组密码结构的关键参数，并简述每一个参数对加密过程的影响。

【解析】 一是数据段长度。数据段长度越长，安全性越高，但增加加密/解密过程的计算复杂性；二是密钥长度。密钥长度越长，安全性越高，但增加加密/解密过程的计算复杂性；三是迭代次数。迭代次数越多，安全性越高，但增加加密/解密过程的计算复杂性；四是子密钥生成算法。子密钥生成算法越复杂，安全性越高，但增加加密/解密过程的计算复杂性；五是迭代函数。迭代函数越复杂，安全性越高，但增加加密/解密过程的计算复杂性。

【例题 3.3】 简述 Feistel 分组密码结构实现扩散和混淆的原理。

【解析】 扩散是尽可能使明文和密钥的每一位能够影响密文的所有位。混淆是尽可能使明文和密钥与密文之间的关系复杂化，即明文与密文之间、密钥和密文之间的统计相关性极小化。混淆主要通过置换过程实现，通过置换将明文随机分布到密文中。扩散主要通过以下过程实现：一是通过子密钥生成函数生成每一次迭代运算使用的子密钥；二是用子密钥异或参与迭代运算的信息，使每一位密钥尽可能地影响到密文的所有位。

【例题 3.4】 假定用户 A 向用户 B 传输消息的过程如图 3.1 所示，其中 A 和 B 是用户 A 和用户 B 的标识符，KA 和 KB 是用户 A 和用户 B 与 KDC 之间的共享密钥。假定用户 H 具有与 KDC 之间的共享密钥 KH，且用户 H 可以嗅探用户 A、用户 B 和 KDC 之间传输的信息，给出用户 H 获得用户 A 发送给用户 B 的消息 M 的过程。

【解析】

(1) 用户 H 嗅探到用户 A 发送给 KDC 的 $E_{KA}(R)$和用户 A 发送给用户 B 的 $E_{KB}(R)$

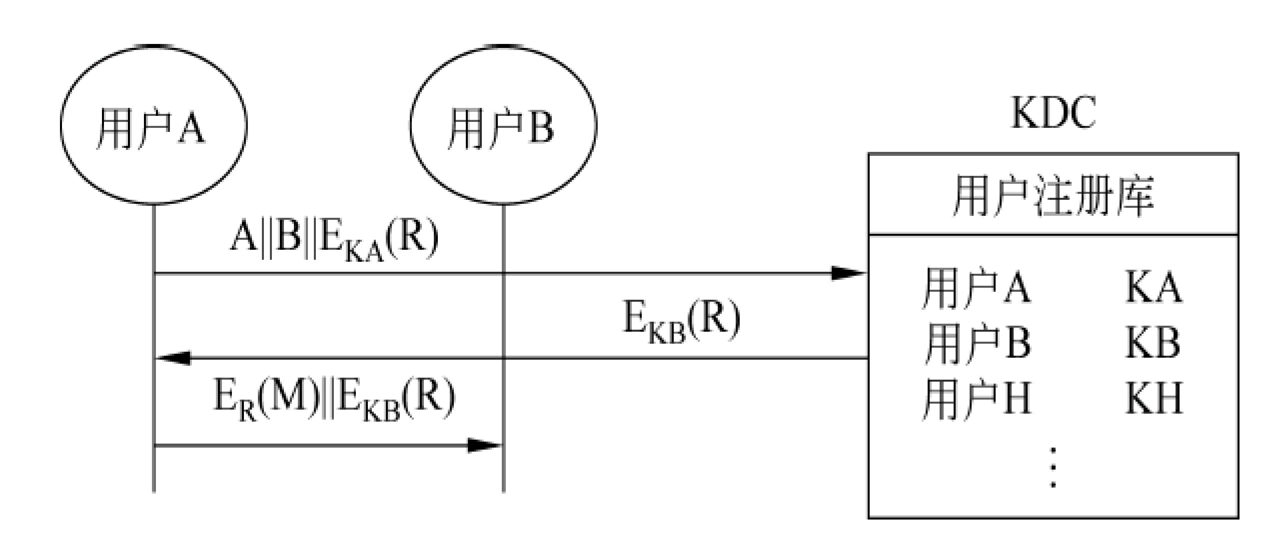


图 3.1 用户 A 向用户 B 传输消息的过程

与 E_R(M)。

(2) 用户 H 向 KDC 发送 A ‖ H ‖ E_{KA}(R),即伪造用户 A 需要向用户 H 加密发送消息的请求。

(3) KDC 向用户 H 发送 E_{KH}(R)。

(4) 用户 H 接收到 E_{KH}(R)后,解密出 R,根据 R 和 E_R(M)解密出 M。

【例题 3.5】 在图 3.2 所示的加密过程中,IV 是初始向量,m_0、m_1、…、m_p 是明文数据段,c_0、c_1、…、c_p 是密文数据段,k 是密钥。回答以下问题。

(1) 给出如图 3.2 所示的加密过程对应的工作模式,并给出加密算法。

(2) 给出如图 3.2 所示的加密过程对应的解密过程,并给出解密算法。

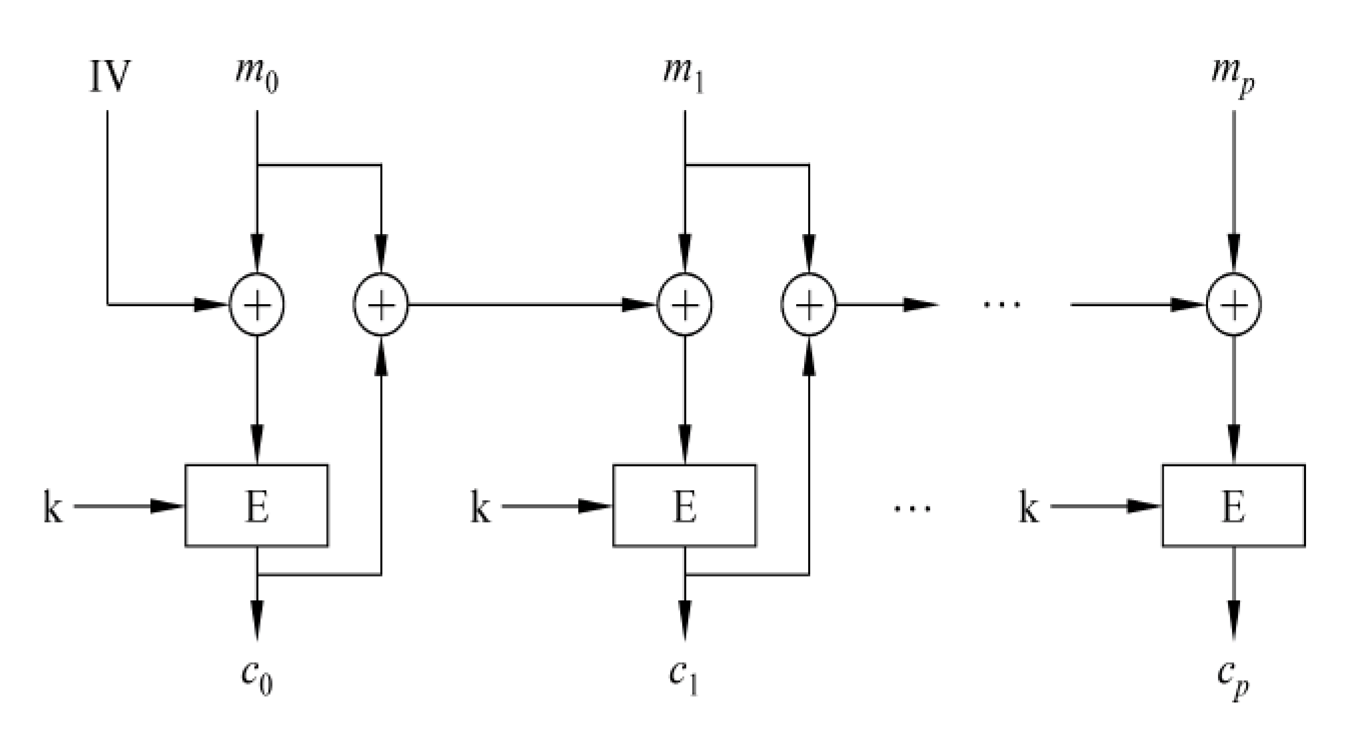


图 3.2 加密过程

(3) 简述这种工作模式的优缺点。

【解析】

(1) 工作模式是明密文链接模式(Plaintext and Ciphertext Block Chaining),加密算法如下。

$$c_0 = E_k(m_0 \oplus IV) \qquad (i=0)$$

$$c_i = E_k(m_{i-1} \oplus c_{i-1} \oplus m_i) \qquad (i=1,2,\cdots,p)$$

(2) 解密过程如图 3.3 所示。解密算法如下。

$$m_0 = D_k(c_0) \oplus IV \qquad (i=0)$$

$$m_i = D_k(c_i) \oplus c_{i-1} \oplus m_{i-1} \qquad (i=1,2,\cdots,p)$$

(3) 优点是对于有规则重复的明文,密文也不会是有规则重复的。缺点是明文或密文中只要发生一位错误,该位错误将影响后续所有的加密或解密结果。这种现象称为错误传播。

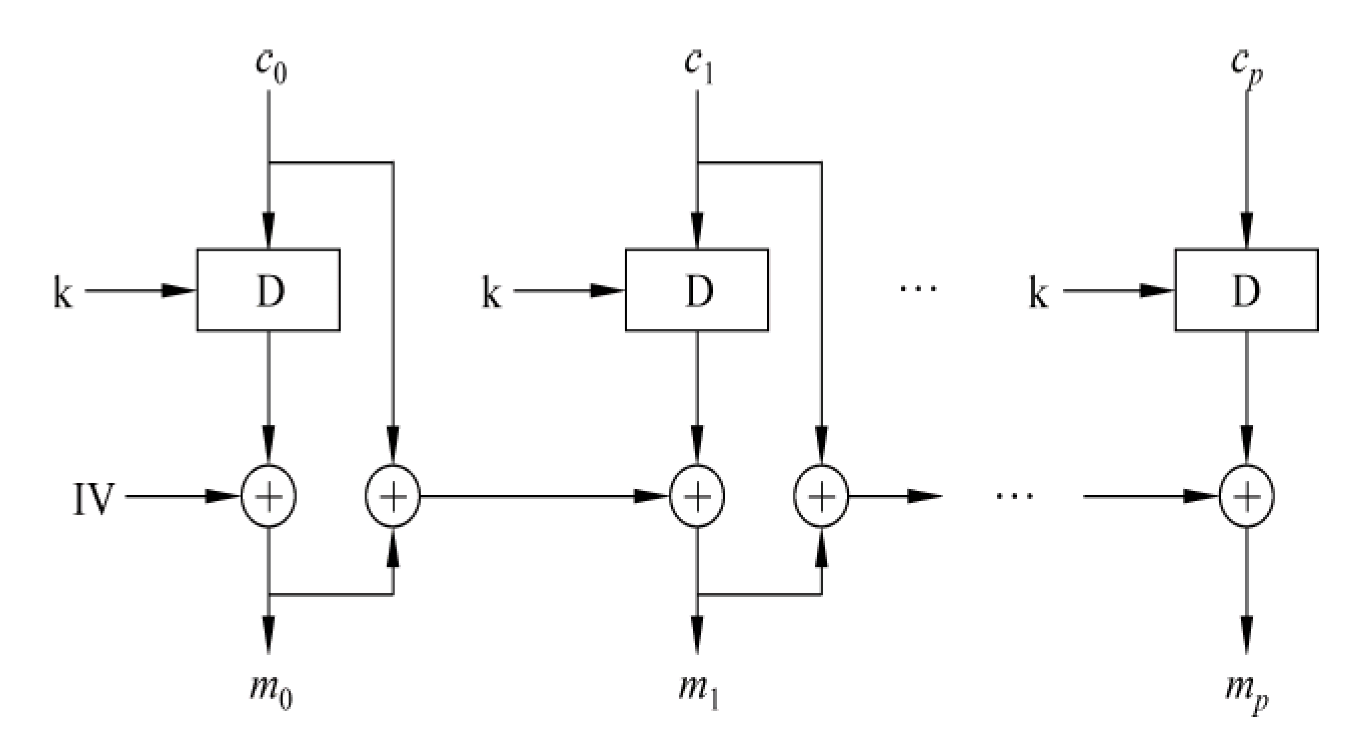


图 3.3　解密过程

3.1.2　计算题解析

【例题 3.6】 完成字符串“this is a good job”恺撒密码加密/解密过程(加密/解密过程不含字符串中的空格)。

【解析】 恺撒密码的加密过程如下：字符串中的每一个字符用字符表中该字符之后的第三个字符替代。因此,完成加密过程后,字符串“this is a good job”对应的密文是“wklv lv d jrrg mre”。恺撒密码的解密过程如下：字符串中的每一个字符用字符表中该字符之前的第三个字符替代。因此,完成解密过程后,字符串“wklv lv d jrrg mre”对应的明文是 “this is a good job”。

【例题 3.7】 假定密钥串是“work”,完成字符串“this is a good job”维吉尼亚密码加密/解密过程(加密/解密过程不含字符串中的空格)。

【解析】 维吉尼亚密码将 26 个字母分别编号,其中 a 的编号为 0,b 的编号为 1,依此类推。密钥串“work”对应的编号分别是“22,14,17,10”,将字符串“this is a good job”以密钥串的长度 4 为单位分段,分为“this isag oodj ob”。加密过程如表 3.1 所示,求出分段后每一段中 4 个字符对应的编号,4 个字符对应的编号分别加上“22,14,17,10”。然后对和进行 26 的模运算,模运算结果就是密文中该字符的编号。表 3.1 中第 2 行所示的是明文字母对应的编号。表 3.1 中第 3 行所示的是对各个明文字母编号增加的值。表 3.1 中第 4 行所示的是对和进行模 26 运算后的结果,即密文字母的编号。表 3.1 中第 5 行所示的是密文字母。因此,完成加密过程后,字符串“this is a good job”对应的密文是“pvzc eg r qkcu tkp”。

表 3.1　加密过程

t	h	i	s	i	s	a	g	o	o	d	j	o	b
19	7	8	18	8	18	0	6	14	14	3	9	14	1
22	14	17	10	22	14	17	10	22	14	17	10	22	14
15	21	25	2	4	6	17	16	10	2	20	19	10	15
p	v	z	c	e	g	r	q	k	c	u	t	k	p

解密过程如表 3.2 所示，将密文字符串以密钥串的长度 4 为单位分段，求出分段后每一段中 4 个字符对应的编号，4 个字符对应的编号分别减去“22，14，17，10”，如果某个字符对应的编号不够减，加上 26 后再进行减运算，得到的差就是明文中该字符的编号。表 3.2 中第 2 行所示的是密文字母对应的编号。表 3.2 中第 3 行所示的是对各个密文字母编号减去的值。表 3.2 中第 4 行所示的是差值，即明文字母的编号。表 3.2 中第 5 行所示的是明文字母。

表 3.2 解密过程

p	v	z	c	e	g	r	q	k	c	u	t	k	p
15	21	25	2	4	6	17	16	10	2	20	19	10	15
22	14	17	10	22	14	17	10	22	14	17	10	22	14
19	7	8	18	8	18	0	6	14	14	3	9	14	1
t	h	i	s	i	s	a	g	o	o	d	j	o	b

【例题 3.8】 如果 8 位数据段的置换规则为{8，5，4，1，7，2，6，3}，求出逆置换规则。假定 8 位数据段是 10011101，给出置换和逆置换过程。

【解析】 置换规则{8，5，4，1，7，2，6，3}表明，置换后的 8 位数据段中的第 1 位是置换前的 8 位数据段中的第 8 位，置换后的 8 位数据段中的第 2 位是置换前的 8 位数据段中的第 5 位，依此类推，置换后的 8 位数据段中的第 8 位是置换前的 8 位数据段中的第 3 位，因此，置换过程如图 3.4 所示。

由于置换规则{8，5，4，1，7，2，6，3}将第 1 位置换成第 4 位，第 2 位置换成第 6 位，第 3 位置换成第 8 位，依此类推，第 8 位置换成第 1 位。因此，逆置换需要将第 4 位置换成第 1 位，第 6 位置换成第 2 位，第 8 位置换成第 3 位，依此类推，第 1 位置换成第 8 位。由此得出逆置换规则为{4，6，8，3，2，7，5，1}。逆置换过程如图 3.5 所示。

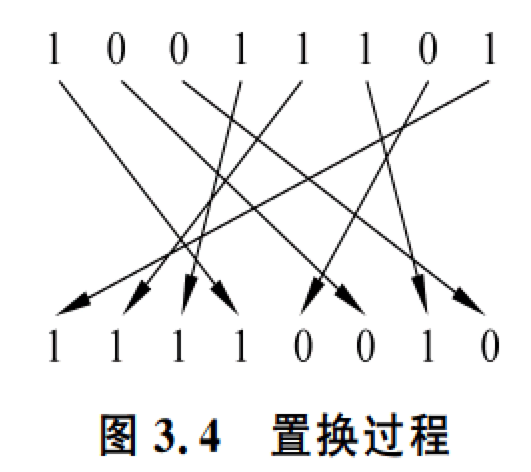


图 3.4 置换过程

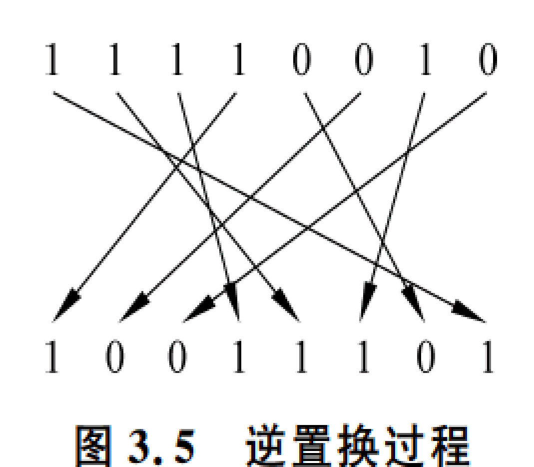


图 3.5 逆置换过程

【例题 3.9】 如果置换规则是{2，4，1，3}，完成字符串“this is a good job”置换密码加密/解密过程(加密/解密过程不含字符串中的空格)。

【解析】 加密过程如下。将字符串“this is a good job”以长度 4 为单位分段，分为“this isag oodj ob□□”，其中□是添加的空格。每一段根据置换规则{2，4，1，3}进行如图 3.6 所示的置换过程。

根据置换规则{2，4，1，3}，求出逆置换规则过程如下，由于置换规则{2，4，1，3}表明，明文数据段中的第 1 个字符置换成密文数据段中的第 3 个字符，因此，逆置换过程需要重新将密文数据段中的第 3 个字符置换成明文数据段中的第 1 个字符，依此类推，将密文数

解密过程如表 3.2 所示，将密文字符串以密钥串的长度 4 为单位分段，求出分段后每一段中 4 个字符对应的编号，4 个字符对应的编号分别减去“22,14,17,10”，如果某个字符对应的编号不够减，加上 26 后再进行减运算，得到的差就是明文中该字符的编号。表 3.2 中第 2 行所示的是密文字母对应的编号。表 3.2 中第 3 行所示的是对各个密文字母编号减去的值。表 3.2 中第 4 行所示的是差值，即明文字母的编号。表 3.2 中第 5 行所示的是明文字母。

表 3.2　解密过程

p	v	z	c	e	g	r	q	k	c	u	t	k	p
15	21	25	2	4	6	17	16	10	2	20	19	10	15
22	14	17	10	22	14	17	10	22	14	17	10	22	14
19	7	8	18	8	18	0	6	14	14	3	9	14	1
t	h	i	s	i	s	a	g	o	o	d	j	o	b

【例题 3.8】 如果 8 位数据段的置换规则为{8,5,4,1,7,2,6,3}，求出逆置换规则。假定 8 位数据段是 10011101，给出置换和逆置换过程。

【解析】 置换规则{8,5,4,1,7,2,6,3}表明，置换后的 8 位数据段中的第 1 位是置换前的 8 位数据段中的第 8 位，置换后的 8 位数据段中的第 2 位是置换前的 8 位数据段中的第 5 位，依此类推，置换后的 8 位数据段中的第 8 位是置换前的 8 位数据段中的第 3 位，因此，置换过程如图 3.4 所示。

由于置换规则{8,5,4,1,7,2,6,3}将第 1 位置换成第 4 位，第 2 位置换成第 6 位，第 3 位置换成第 8 位，依此类推，第 8 位置换成第 1 位。因此，逆置换需要将第 4 位置换成第 1 位，第 6 位置换成第 2 位，第 8 位置换成第 3 位，依此类推，第 1 位置换成第 8 位。由此得出逆置换规则为{4,6,8,3,2,7,5,1}。逆置换过程如图 3.5 所示。

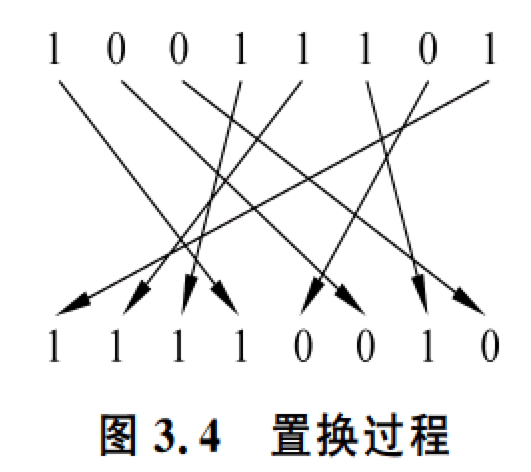


图 3.4　置换过程

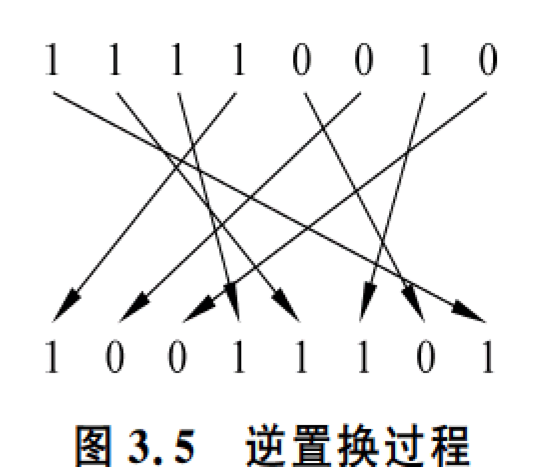


图 3.5　逆置换过程

【例题 3.9】 如果置换规则是{2,4,1,3}，完成字符串“this is a good job”置换密码加密/解密过程（加密/解密过程不含字符串中的空格）。

【解析】 加密过程如下。将字符串“this is a good job”以长度 4 为单位分段，分为“this isag oodj ob□□”，其中□是添加的空格。每一段根据置换规则{2,4,1,3}进行如图 3.6 所示的置换过程。

根据置换规则{2,4,1,3}，求出逆置换规则过程如下，由于置换规则{2,4,1,3}表明，明文数据段中的第 1 个字符置换成密文数据段中的第 3 个字符，因此，逆置换过程需要重新将密文数据段中的第 3 个字符置换成明文数据段中的第 1 个字符，依此类推，将密文数

据段中的第1个字符置换成明文数据段中的第2个字符，将密文数据段中的第4个字符置换成明文数据段中的第3个字符，将密文数据段中的第2个字符置换成明文数据段中的第4个字符，由此得出逆置换规则是{3,1,4,2}。逆置换过程如图3.7所示。

this　isag　oodj　ob□□
hsti　sgia　ojod　b□o□

图3.6　置换过程

hsti　sgia　ojod　b□o□
this　isag　oodj　ob□□

图3.7　逆置换过程

【例题3.10】 假设十六进制表示的64位密钥k=0f1571c947d9e859，P1和P2选位置换规则分别如表3.3和表3.4所示。分别求出DES参与第一次迭代运算的子密钥k_1和参与第二次迭代运算的子密钥k_2。

表3.3　P1选位置换规则

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

表3.4　P2选位置换规则

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

【解析】 二进制表示的64位密钥k如下。

00001111 00010101 01110001 11001001 01000111 11011001 11101000 01011001

64位密钥k从左到右的编号依次为1～64，表3.3所示的P1选位置换规则表明，28位C_0的第1位是64位密钥k的第57位，第2位是64位密钥k的第49位，第28位是64位密钥k的第36位。28位D_0的第1位是64位密钥k的第63位，第2位是64位密钥k的第55位，第28位是64位密钥k的第4位。按照如表3.3所示的P1选位置换规则完成置换运算后，得到的28位C_0和D_0分别如下所示。

$$C_0=01101000\quad 11111100\quad 01000100\quad 1010$$

$$D_0=00010001\quad 00010011\quad 11101001\quad 0110$$

分别将C_0和D_0循环左移1位，得到以下结果。

$$C_1=1101000111111000100010010100$$

$$D_1=0010001000100111110100101100$$

C_1和D_1合并为如下56位的C_1D_1，56位的C_1D_1从左到右的编号依次为1～56。

C_1D_1=1101000111　1110001000　1001010000　1000100010　0111110100　101100

表3.4所示的P2选位置换规则表明，48位k_1的第1位是56位C_1D_1的第14位，第

2 位是 56 位 C_1D_1 的第 17 位，第 48 位是 56 位 C_1D_1 的第 32 位。按照如表 3.4 所示的 P2 选位置换规则完成置换运算后，得到如下参与第一次迭代运算的子密钥 k_1。

k_1＝011110 000011 001111 000011 001000 001101 101001 110000

分别将 C_1 和 D_1 循环左移 1 位，得到以下结果。

$$C_2=1010001111110001000100101001$$

$$D_2=0100010001001111101001011000$$

C_2 和 D_2 合并为如下 56 位的 C_2D_2，56 位的 C_2D_2 从左到右的编号依次为 1～56。

$C_2\ D_2$＝1010001111 1100010001 0010100101 0001000100 1111101001 011000

表 3.4 所示的 P2 选位置换规则表明，48 位 k_2 的第 1 位是 56 位 C_2D_2 的第 14 位，第 2 位是 56 位 C_2D_2 的第 17 位，第 48 位是 56 位 C_2D_2 的第 32 位。按照如表 3.4 所示的 P2 选位置换规则完成置换运算后，得到如下参与第二次迭代运算的子密钥 k_2。

k_2＝001010 110001 101001 110100 110010 100100 100011 011000

【例题 3.11】 根据 Diffie-Hellman 计算密钥机制，假设素数 $q=11$，原根 $\alpha=2$，完成下列计算。

(1) 证明 2 是素数 11 的原根。

(2) 用户 A 公钥 $Y_A=9$，计算私钥 X_A。

(3) 用户 B 公钥 $Y_B=3$，计算共享密钥 K。

【解析】

(1) 2 mod 11＝2，2^2 mod 11＝4，2^3 mod 11＝8，2^4 mod 11＝5，2^5 mod 11＝10，2^6 mod 11＝9，2^7 mod 11＝7，2^8 mod 11＝3，2^9 mod 11＝6，2^{10} mod 11＝1。即{2 mod 11，2^2 mod 11，…，2^{10} mod 11}包含了 1～10 的所有整数。由此证明，2 是素数 11 的原根。

(2) 由于 $YA=\alpha^{XA} \bmod p$，根据 2^6 mod 11＝9 得出，当公钥 $Y_A=9$ 时，私钥 $X_A=6$。

(3) $K=YB^{XA} \bmod p=3^6 \bmod 11=3$。

需要说明的是，当 p 的二进制数位数超过 768 位时，根据现有计算能力，通过公钥 Y_A 求出对应的私钥 X_A 是不可能的。

【例题 3.12】 根据以下值，给出 RSA 加密/解密运算过程。

(1) $p=3, q=11, e=7, M=5$。

(2) $p=5, q=11, e=3, M=9$。

(3) $p=7, q=11, e=17, M=8$。

【解析】

(1) $n=p\times q=3\times 11=33$。

$\Phi(n)=(p-1)\times(q-1)=2\times 10=20$。

根据$(7\times d) \bmod 20=1$，求出 $d=3$。

$c=M^e \bmod n=5^7 \bmod 33=14$。

$M=c^d \bmod n=14^3 \bmod 33=5$。

(2) $n=p\times q=5\times 11=55$。

$\Phi(n)=(p-1)\times(q-1)=4\times 10=40$。

根据$(3\times d) \bmod 40=1$，求出 $d=27$。

$c = M^e \bmod n = 9^3 \bmod 55 = 14$。

$M = c^d \bmod n = 14^{27} \bmod 55 = 9$。

(3) $n = p \times q = 7 \times 11 = 77$。

$\Phi(n) = (p-1) \times (q-1) = 6 \times 10 = 60$。

根据 $(17 \times d) \bmod 60 = 1$，求出 $d = 53$。

$c = M^e \bmod n = 8^{17} \bmod 77 = 57$。

$M = c^d \bmod n = 57^{53} \bmod 77 = 8$。

【例题 3.13】 假定有 n 个节点，需要实现两两节点之间的加密通信，分别计算出对称密钥体制和公开密钥体制下需要的总的密钥数和每一个节点需要保持的密钥数。

【解析】 在对称密钥体制下，每一对节点需要有独立的对称密钥，n 个节点可以组合成 $n \times (n-1)/2$ 对节点，因此，密钥总数 $= n \times (n-1)/2$。每一个节点需要与其他 $n-1$ 个不同的节点通信，因此，需要保持 $n-1$ 个不同的对称密钥。

在公开密钥体制下，每一个节点需要一对密钥，即公钥和私钥对，n 个节点的密钥总数 $= 2 \times n$。

每一个节点需要与其他 $n-1$ 个不同的节点通信，因此，需要保持这些节点对应的 $n-1$ 个不同的公钥。为了解密其他节点发送给它的密文，需要保持自己的私钥。

3.2　选择题分析

(1) 关于密码技术，以下哪一项描述是错误的？(　　)

A. 密码学包括密码编码学和密码分析学两门学科

B. 对称密钥密码体制也称为单密钥密码体制或传统密码体制，基本特征是发送方和接收方共享相同的密钥，即加密密钥与解密密钥相同

C. 密码体制的安全既依赖于对密钥的保密，又依赖于对算法的保密

D. 对称密钥加密算法不易实现数字签名，限制了它的应用范围

答案：C

【分析】 现代密码体制的 Kerckhoff's 原则是：所有加密/解密算法都是公开的，保密的只是密钥。

(2) 好的加密算法只能采用以下哪一项方法破译密文？(　　)

A. 穷举　　B. 数学分析

C. 明文和密文对照　　D. 分析密文规律

答案：A

【分析】 好的加密算法除了逐个尝试密钥空间中的所有密钥，不应有其他破译密文的有效方法。

(3) 安全的加密算法具有以下哪一项特点？(　　)

A. 只能用穷举法破译密文　　B. 密钥长度足够

C. 经得住网格计算考验　　D. 以上全部

答案：D

【分析】 只能以穷举法破译密文说明加密算法可靠，密钥长度足够说明穷举法破译密文所需的时间很长，经得住网格计算考验说明目前还没有找到以较小的代价用穷举法破译密文的方法。

(4) 安全的加密算法满足以下哪一项条件？(　　)

A. 无法破译密文　　B. 破译密文的成本超过密文价值

C. 破译密文时间超过密文有效期　　D. B 或 C

答案：D

【分析】 不存在无法破译的密文，区别在于破译密文付出的代价和所需的时间。

(5) 在网络安全中，加密算法的用途包含以下哪一项？(　　)

A. 加密信息　　B. 信息完整性检测

C. 用户身份鉴别　　D. 以上全部

答案：D

【分析】 在网络安全中，加密算法不再仅仅用于加密数据。

(6) 关于加密，以下哪一项描述是错误的？(　　)

A. 加密是明文至密文的转换过程

B. 加密必须是可逆的

C. 只能通过加密的逆过程完成密文至明文的转换过程

D. 可以直接从密文导出明文

答案：D

【分析】 虽然通过加密的逆过程可以完成密文至明文的转换过程，即解密过程，但完成解密过程需要两个前提：一是掌握与加密算法对应的解密算法；二是掌握与加密密钥对应的解密密钥。这两个前提是无法直接通过密文导出的。

(7) 对于 $c=\mathrm{E}(m,\mathrm{k}_e)$($c$ 是密文，E 是加密算法，m 是明文，k_e 是加密密钥)，以下哪一项描述是错误的？(　　)

A. 无法根据 c 导出 m　　B. 无法根据 c 和 E 导出 m

C. 无法根据 c、E 和 m 导出 k_e　　D. 无法根据 E、k_e 和 c 导出 m

答案：D

【分析】 现代密码体制的加密/解密算法都是公开的，因此，可以根据 E 导出解密算法 D。对于对称密钥体制，解密密钥 k_d 等于加密密钥 k_e，因此，在对称密钥体制下，可以根据 E、k_e 和 c 导出 m。

(8) 关于对称密钥体制，以下哪一项描述是错误的？(　　)

A. 加密/解密算法是公开的

B. 加密密钥等于解密密钥

C. 保密密钥是唯一的安全保证

D. 可以安全地基于网络分发密钥

答案：D

【分析】 由于密钥不能被第三方窃取，因此，基于网络分发密钥是存在安全隐患的。

(9) 关于对称密码，以下哪一项描述是错误的？(　　)

A. 加密/解密处理速度快　　B. 加密/解密使用的密钥相同

C. 密钥管理和分发简单　　D. 数字签名困难

答案：C

【分析】 对称密码的主要缺陷是密钥管理和分发困难。

(10) 关于非对称密钥体制，以下哪一项描述是错误的？(　　)

A. 加密/解密算法是公开的　　B. 加密密钥不等于解密密钥

C. 无法通过加密密钥导出解密密钥　　D. 需要基于网络分发解密密钥

答案：D

【分析】 由于只有接收端才需要解密密钥，因此，不存在分发解密密钥的问题。

(11) 关于非对称密钥体制，以下哪一项描述是错误的？(　　)

A. 基于难解问题设计密钥是非对称密钥设计的主要思想

B. 公开密钥易于实现数字签名

C. 公开密钥的优点在于从根本上克服了对称密钥分发上的困难

D. 公开密钥加密算法安全性高，与对称密钥加密算法相比，更加适合于数据加密

答案：D

【分析】 公开密钥加密算法和对称密钥加密算法的安全性都是有保障的，但公开密钥加密算法的计算复杂性远高于对称密钥加密算法，因此，公开密钥加密算法并不适合于数据加密。

(12) 密码分析学是研究密码破译的科学，在密码分析过程中，以下哪一项是破译密文的关键？(　　)

A. 截获密文

B. 截获密文并获得密钥

C. 截获密文，了解加密算法和解密算法

D. 截获密文，获得密钥并了解解密算法

答案：D

【分析】 解密的关键是获得密钥和解密算法。

(13) 通过无线电侦听获取密文，并对密文进行破译属于以下哪种攻击？(　　)

A. 唯密文攻击　　B. 已知明文攻击

C. 选择明文攻击　　D. 选择密文攻击

答案：A

【分析】 在破译密文时，仅仅截获若干密文。

(14) 已经发现有间谍活动，且能够侦听间谍发出的无线电，故意发生某个间谍关注的事件，且侦听到间谍汇报该事件的密文。这种情况属于以下哪种攻击？(　　)

A. 唯密文攻击　　B. 已知明文攻击

C. 选择明文攻击　　D. 选择密文攻击

答案：B

【分析】 解析密钥时，密文对应的明文是知道的。

(15) 黑客攻击过程如图 3.8 所示，黑客终端 1 根据解析密钥要求产生并向终端 A 发送明文，黑客终端 2 侦听到 AP 发送给终端 A 的密文。这种情况属于以下哪种攻击？(　　)

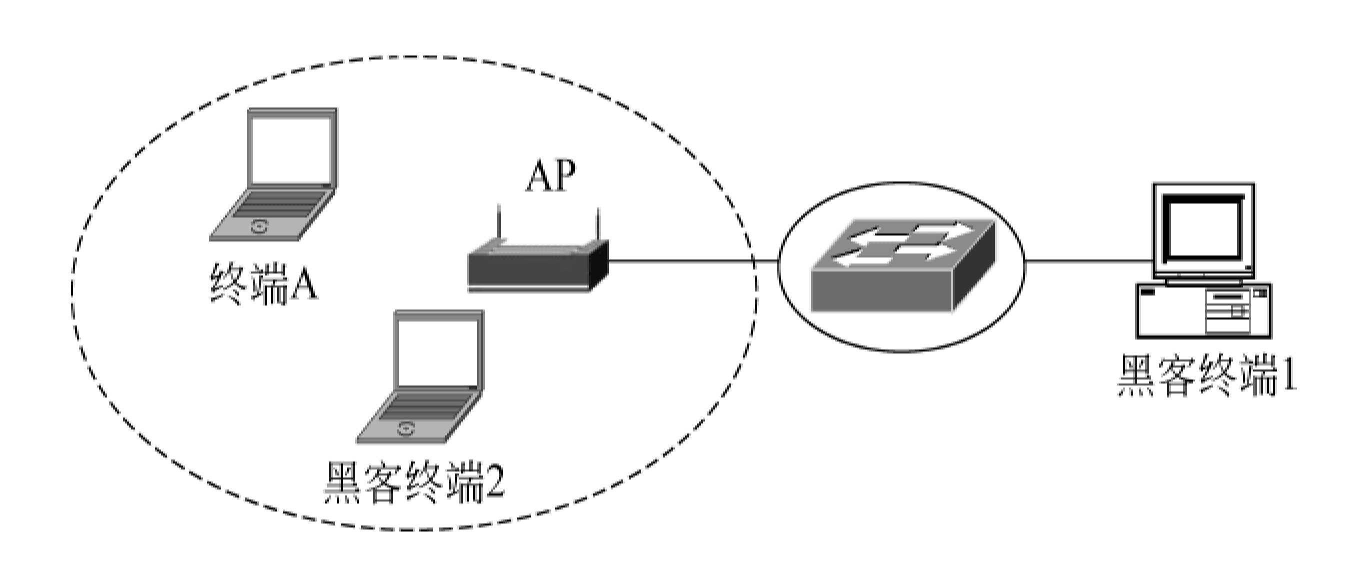


图 3.8　黑客攻击过程

A. 唯密文攻击　　B. 已知明文攻击

C. 选择明文攻击　　D. 选择密文攻击

答案：C

【分析】 解析密钥时，密文对应的明文是知道的，且明文内容是由黑客指定的。

(16) 黑客攻击过程如图 3.9 所示，黑客终端 2 冒充终端 A 发送 MAC 帧，MAC 帧中的密文是黑客终端 2 根据解析密钥要求指定的，AP 将解密后的明文发送给黑客终端 1。这种情况属于以下哪种攻击？(　　)

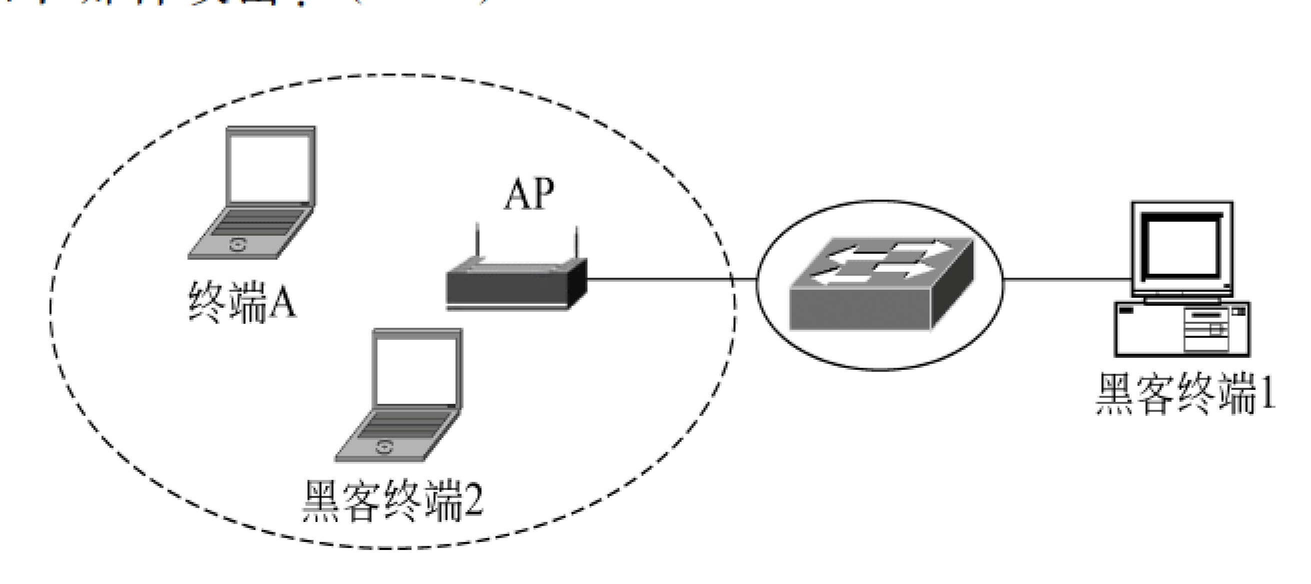


图 3.9　黑客攻击过程

A. 唯密文攻击　　B. 已知明文攻击

C. 选择明文攻击　　D. 选择密文攻击

答案：D

【分析】 解析密钥时，密文对应的明文是知道的，且密文内容是由黑客指定的。

(17) 关于分组密码体制，以下哪一项描述是错误的？(　　)

A. 需要对明文分段　　B. 密文长度与明文长度相同

C. 密文与明文是一对一映射　　D. 密钥长度与密文长度相同

答案：D

【分析】 分组密码体制下，密钥长度与密文长度之间没有严格的相互制约关系。

(18) 关于分组密码体制，以下哪一项描述是正确的？(　　)

A. 分段后的明文数据段长度可以任意，密钥长度可以任意

B. 分段后的明文数据段长度可以任意，密钥长度需要足够大

C. 分段后的明文数据段长度需要足够大，密钥长度可以任意

D. 分段后的明文数据段长度需要足够大，密钥长度需要足够大

答案：D

【分析】 分段后的明文数据段长度和密钥长度一起确定该分组密码体制允许存在的明文与密文之间的映射数量。

(19) 关于 DES,以下哪一项描述是正确的?(　　)

A. 密钥 64 位　　B. 密钥 56 位　　C. 密钥 128 位　　D. 密钥 32 位

答案：B

【分析】 DES 真正的密钥长度是 56 位。

(20) 关于 DES,以下哪一项描述是正确的?(　　)

A. 明文数据段长度 64 位,密文长度 56 位

B. 明文数据段长度 56 位,密文长度 64 位

C. 明文数据段长度 56 位,密文长度 56 位

D. 明文数据段长度 64 位,密文长度 64 位

答案：D

【分析】 DES 明文数据段长度和密文长度都是 64 位。任意长度的明文需要分割为 64 位长度的数据段。

(21) 在 DES 加密过程中,需要进行 16 轮加密,每一轮的子密钥长度是(　　)。

A. 16　　B. 32　　C. 48　　D. 64

答案：C

【分析】 子密钥长度是 48 位。

(22) 关于 DES,以下哪一项描述是正确的?(　　)

A. 只能通过穷举法解析密钥

B. 在现有计算能力下,密钥集已经大到无法解析密钥的程度

C. 在现有计算能力下,完成一次加密运算的过程需要很长时间

D. 可以通过有限的密文和明文对解析出密钥

答案：A

【分析】 DES 加密算法的复杂性可以保证只能通过穷举法解析密钥。但随着计算机运算速度的提高,完成一次加密运算需要的时间越来越短。云计算的应用使个人获得的计算能力越来越大,暴力破解 DES 密钥已经成为可能。

(23) 如果替代规则表如表 3.5 所示,则当 S 盒输入 110011 时,输出的是以下哪一个值?(　　)

表 3.5　替代规则表

00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

A. 0010　　B. 1010　　C. 1011　　D. 0011

答案：C

【分析】 假定 6 位数据段表示成 $a_1a_2a_3a_4a_5a_6$，将 6 位数据段分成两部分：a_1a_6 和 $a_2a_3a_4a_5$，两位 a_1a_6 用于在表 3.5 对应的 4 行替代编码中选择 1 行，4 位 $a_2a_3a_4a_5$ 用于在通过 a_1a_6 选定的这一行的 16 个 4 位替代编码中选择一个替代编码。当输入的 6 位数据段 $a_1a_2a_3a_4a_5a_6=110011$ 时，用 11 选定对应的第 4 行，用 1001 选择第 4 行中第 9 个替代编码，这里是十进制数 11，即 1011。

(24) 两个密钥三重 DES 加密，即 $c=E_{K1}(D_{K2}(E_{K1}(p)))$，K1≠K2，其有效的密钥长度是(　　)。

A. 56　　B. 128　　C. 168　　D. 112

答案：D

【分析】 每个 DES 密钥的有效长度是 56 位，两个 DES 密钥的有效长度是 112 位。

(25) 关于 AES，以下哪一项描述是错误的？(　　)

A. 只能通过穷举法解析密钥

B. 在现有计算能力下，密钥集已经大到无法解析密钥的程度

C. 在现有计算能力下，完成一次加密运算的过程需要很长时间

D. 无法通过有限的密文和明文对解析出密钥

答案：C

【分析】 由于 AES 加密算法的复杂性和数据段长度都比 DES 高，因此，AES 完成一次加密运算的过程需要的时间大于 DES，但由于现代计算机的计算能力确实很强，AES 完成一次加密运算的过程所需要的时间不会很长。在现有计算能力下，无法暴力破解 AES 密钥的主要原因是 AES 的密钥集很大。

(26) 关于 AES 的密钥长度，以下哪一项描述是错误的？(　　)

A. 128　　B. 192　　C. 256　　D. 64

答案：D

【分析】 AES 的密钥长度不能是 64。

(27) 关于 AES，以下哪一项描述是正确的？(　　)

A. 明文数据段长度 64 位，密文长度 64 位

B. 明文数据段长度 128 位，密文长度 64 位

C. 明文数据段长度 64 位，密文长度 128 位

D. 明文数据段长度 128 位，密文长度 128 位

答案：D

【分析】 AES 明文数据段长度和密文长度都是 128 位。任意长度的明文需要分割为 128 位长度的数据段。

(28) 以下哪一项描述是错误的？(　　)

A. 在电码本模式下，有规律重复的明文产生有规律重复的密文

B. 在加密分组链接模式下，有规律重复的明文不会产生有规律重复的密文

C. 在计数器模式下，有规律重复的明文不会产生有规律重复的密文

D. 在计数器模式下，发送端和接收端只需相同的密钥

答案：D

【分析】 在计数器模式下，发送端和接收端不仅需要相同的密钥，还需要同步计数器值。

(29) 关于实际流密码体制的缺陷，以下哪一项描述是错误的？(　　)

A. 密钥集是有限的

B. 密钥之间无法做到没有任何相关性

C. 发送端和接收端必须同步密钥

D. 加密算法复杂性不够

答案：D

【分析】 流密码体制的安全性依赖以下因素：一是密钥集足够大，每一次加密运算使用不同的密钥；二是在密钥集中随机选取密钥，密钥之间不存在任何相关性。由于“一次一密”，因此对加密算法的复杂性没有要求。

(30) 关于WEP加密机制的缺陷，以下哪一项描述是错误的？(　　)

A. 用伪随机数生成器产生密钥

B. 作为随机数种子一部分的原始密钥k是不变的

C. 密钥集中的密钥数$\leqslant 2^{24}$

D. 原始密钥k的长度只能是40或104

答案：D

【分析】 WEP采用流密码体制的加密机制，其安全性主要取决于密钥集的大小和密钥之间的相关性。由于计算一次性密钥时，原始密钥k是不变的，因此，原始密钥k的长度对密钥集的大小和密钥之间的相关性影响不大。当然，原始密钥k的长度越大，越难通过伪随机数生成器产生的一次性密钥解析出原始密钥k。

(31) 关于集中式密钥分配过程的缺陷，以下哪一项描述是错误的？(　　)

A. 需要事先约定用户和KDC之间的主密钥

B. 更换用户和KDC之间的主密钥比较麻烦

C. 通信双方必须注册在同一个KDC

D. 获取通信双方使用的会话密钥比较困难

答案：D

【分析】 采用集中式密钥分配过程带来的主要优点是：方便通信双方获取通信时使用的会话密钥。

(32) 关于Diffie-Hellman密钥交换算法，以下哪一项描述是错误的？(　　)

A. 用于同步网络中任何两个终端之间的密钥

B. 交换的随机数以明文方式传输

C. 无法通过截获交换的随机数导出密钥

D. 可以抵御中间人攻击

答案：D

【分析】 Diffie-Hellman密钥交换算法无法抵御中间人攻击，因此，要么交换随机数时提供完整性检测功能，要么双方具有检测对方使用的密钥的功能。

(33) 关于 Diffie-Hellman 密钥交换算法,以下哪一项描述是错误的?(　　)

A. 安全性取决于大素数 p 的位数

B. 知道大素数 p、原根 α 和相互交换的随机数 $Y=\alpha^X \bmod p$,无法导出 X

C. 常用的大素数 p 的位数超过 768 位

D. 大素数 p 的位数越大越好

答案:D

【分析】 当大素数 p 的位数较大时,无论是计算相互交换的随机数的过程,还是根据相互交换的随机数计算密钥的过程,都是计算复杂性很大的计算过程,因此,正确的做法是,在保证安全性的前提下,选择合适的大素数 p 的位数。

(34) 关于公开密钥加密算法,以下哪一项描述是错误的?(　　)

A. 无法根据公钥 PK 推导出私钥 SK

B. 无法根据 PK 和密文 $c=E_{PK}(m)$推导出明文 m

C. 公钥 PK 和私钥 SK 是成对的

D. 只能用公钥 PK 和加密算法将明文转换成密文

答案:D

【分析】 明文转换成密文是一种变换过程,且这种变换过程是可逆的。因此,用解密算法和私钥 SK 对明文进行解密运算的过程($D_{SK}(m)$)也是一种变换过程,且这种变换过程是可逆的($E_{PK}(D_{SK}(m))=m$)。因此,用解密算法和私钥 SK 对明文进行解密运算的过程也是将明文转换成密文的过程,且可以用公钥 PK 和加密算法将密文还原成明文。

(35) 关于 RSA 加密算法,以下哪一项描述是错误的?(　　)

A. 公钥和私钥不同

B. 无法根据公钥推导出私钥

C. 密文和明文等长

D. 可靠性基于大数因子分解困难的事实

答案:C

【分析】 RSA 加密运算不用替代和置换,明文和密文长度之间关系是变化的,一般不会相同。

(36) 关于 RSA 公开密钥加密算法,以下哪一项描述是错误的?(　　)

A. $n=p\times q$,p 和 q 是两个大素数

B. 欧拉函数 $\Phi(n)=(p-1)\times(q-1)$

C. 根据 e 和 $\Phi(n)$可以计算出满足等式 $ed \bmod \Phi(n)=1$ 的 d

D. 根据 e 和 n 可以计算出满足等式 $ed \bmod \Phi(n)=1$ 的 d

答案:D

【分析】 根据 e 计算出满足等式 $ed \bmod \Phi(n)=1$ 的 d 时,需要知道 $\Phi(n)$。计算 $\Phi(n)$时,需要知道 p 和 q。当 n 足够大时,无法根据 n 得出 p 和 q,且使 $n=p\times q$。

(37) RSA 公钥密码体制中,假定公钥为$(e,n)=(13,35)$,则私钥 d 是(　　)。

A. 11　　B. 13　　C. 15　　D. 17

答案：B

【分析】 $n=35$，说明两个素数 $p=5$，$q=7$，$\Phi(n)=(p-1)\times(q-1)=4\times6=24$。$e=13$，根据$(13\times d)\bmod 24=1$，求出 $d=13$。

(38) 利用公开密钥算法进行数据加密时，采用的方式是(　　)。

A. 发送方用公开密钥加密，接收方用公开密钥解密

B. 发送方用私有密钥加密，接收方用私有密钥解密

C. 发送方用公开密钥加密，接收方用私有密钥解密

D. 发送方用私有密钥加密，接收方用公开密钥解密

答案：C

【分析】 一是公钥是公开的，私钥是保密的；二是只能由接收方解密。因此，只能是发送方用公开密钥加密，接收方用私有密钥解密。

(39) 关于对称密钥体制和非对称密钥体制结合，以下哪一项描述是正确的？(　　)

A. 用对称密钥加密算法加密数据，用非对称密钥加密算法加密对称密钥

B. 用对称密钥加密算法加密非对称密钥，用非对称密钥加密算法加密数据

C. 只用非对称密钥加密算法加密数据

D. 只用对称密钥加密算法加密数据

答案：A

【分析】 结合对称密钥体制和非对称密钥体制优势的做法是：用对称密钥加密算法加密数据，用非对称密钥加密算法加密对称密钥，这样做既减少了计算量，又解决了对称密钥分发困难的问题。

(40) 数字信封技术能够实现以下哪一项功能？(　　)

A. 对发送者和接收者的身份进行认证

B. 保证数据在传输过程中的安全性

C. 防止交易中的抵赖发生

D. 隐藏发送者的身份

答案：B

【分析】 数字信封可以用对称密钥加密算法加密数据，用非对称密钥加密算法加密对称密钥。

(41) A 方有一对密钥(公钥 PKA，私钥 SKA)，B 方有一对密钥(公钥 PKB，私钥 SKB)，如果 A 方向 B 方发送密文 $C=\mathrm{E}_{\mathrm{PKB}}(\mathrm{D}_{\mathrm{SKA}}(M))$。B 方的解密方案是(　　)。

A. $\mathrm{D}_{\mathrm{SKB}}(\mathrm{E}_{\mathrm{PKA}}(C))$　　B. $\mathrm{E}_{\mathrm{PKA}}(\mathrm{E}_{\mathrm{PKB}}(C))$

C. $\mathrm{E}_{\mathrm{PKA}}(\mathrm{D}_{\mathrm{SKB}}(C))$　　D. $\mathrm{D}_{\mathrm{SKB}}(\mathrm{D}_{\mathrm{SKB}}(C))$

答案：C

【分析】 $\mathrm{E}_{\mathrm{PKA}}(\mathrm{D}_{\mathrm{SKB}}(C))=\mathrm{E}_{\mathrm{PKA}}(\mathrm{D}_{\mathrm{SKB}}(\mathrm{E}_{\mathrm{PKB}}(\mathrm{D}_{\mathrm{SKA}}(M))))=\mathrm{E}_{\mathrm{PKA}}(\mathrm{D}_{\mathrm{SKA}}(M))=M$。

(42) 公开密钥密码体制的含义是(　　)。

A. 将所有密钥公开　　B. 将秘密密钥公开，公开密钥保密

C. 将公开密钥公开，秘密密钥保密　　D. 两个密钥相同

答案：C

【分析】 公开密钥密码体制分配两个密钥：公开密钥和秘密密钥。公开密钥公开，秘密密钥保密。

3.3 名词解释

(1) 加密

明文至密文的转换过程。

(2) 解密

密文至明文的转换过程。

(3) 对称密钥体制

加密密钥等于解密密钥的密钥体制。

(4) 非对称密钥体制

加密密钥不等于解密密钥，且无法由一个密钥直接导出另一个密钥的密钥体制。

(5) 分组密码体制

一种将明文分割为固定长度的数据段，每一段数据段独立完成加密过程，产生与数据段长度相等的密文，加密/解密算法足够复杂，以至于无法通过有限的明文和密文对解析出密钥的密码体制。

(6) 流密码体制

一种采用"一次一密"，且密钥必须在足够大的密钥集中随机产生，确保密钥之间没有相关性，攻击者无法根据已知的有限密钥序列推导出下一次用于加密运算的密钥，但对加密/解密算法的复杂性没有要求的密码体制。

(7) 替代运算

将数据段中的二进制数分段，每一段二进制数用对应的编码代替。

(8) 置换运算

按照置换规则重新排列数据段中二进制数的顺序。

(9) DES

一种分组密码体制的加密算法，明文数据段长度和密文长度为 64 位，输入密钥长度为 64 位，但只有 56 位是真正密钥。

(10) AES

一种分组密码体制的加密算法，明文数据段长度和密文长度为 128 位，密钥长度可以是 128、192 或 256 位。

(11) 电码本模式

一种分组密码操作模式，加密时，每一段明文独立映射成密文；解密时，每一段密文独立映射成明文。

(12) 加密分组链接模式

一种分组密码操作模式，加密运算模块的输入不是分割明文后产生的数据段 m_i，而是数据段 m_i 和前一次加密运算后的结果 c_{i-1} 异或运算后的结果。m_i 是第 i 段数据段，c_{i-1} 是第 $i-1$ 段数据段对应的密文。

(13) 计数器模式

一种分组密码操作模式，计数器的位数等于分组加密算法要求的明文段长度，不同的明文段对应着不同的计数器，加密算法只对计数器值进行加密，加密运算结果和明文段进行异或运算，异或运算结果就是该明文段对应的密文。

(14) KDC

在集中式密钥分配过程中，为通信双方分配会话密钥的机构。

(15) Diffie-Hellman 密钥交换算法

一种终端之间通过交换随机数实现密钥同步的算法。交换的随机数可以以明文的方式经过网络传输。

(16) RSA

一种公开密钥加密算法，公钥 PK=(e,n)，私钥 SK=(d,n)，且无法通过 n 和 e 导出 d。

(17) 数字信封

在用对称密钥加密算法对数据进行加密/解密运算，用公开密钥加密算法对密钥进行加密/解密运算的应用方式下，用公开密钥算法和公钥加密对称密钥加密算法使用的密钥得到的密文。

第4章 报文摘要算法

4.1 例题解析

【例题4.1】 如果计算检错码的算法是检验和，假定数据 D=“1234567”，附加信息 C 是字符串中每一个字符的 ASCII 码按照反码加法运算规则累加后的结果。改变数据，且使根据改变后的数据计算出的附加信息等于根据数据 D=“1234567”计算出的附加信息。

【解析】 当数据 D=“1234567”时，附加信息 $C=00110001+00110010+00110011+00110100+00110101+00110110+00110111=01101101$。

如果数据 D'=“1334566”，附加信息 $C'=00110001+00110011+00110011+00110100+00110101+00110110+00110110=01101101$。

由此可见，如果检错码算法是检验和，对于数据 D=“1234567”，很容易找到数据 D'=“1334566”，$D \neq D'$，但检错码是相同的。

【例题4.2】 如果计算检验和的算法是 CRC，假定数据是 10110011，生成函数 $G(x)=X^4+X+1=10011$。改变数据，且使根据改变后的数据计算出的附加信息等于根据数据 10110011 计算出的附加信息。

【解析】 当数据=10110011 时，$R(X)=X^4 \times M(X)/G(X)=101100110000/10011=0100$。

如果数据=00001101，$R'(X)=X^4 \times M'(X)/G(X)=000011010000/10011=0100$。

由此可见，如果检错码算法是 CRC，对于数据 $M(X)=10110011$，很容易找到数据 $M'(X)=00001101$，$M(X) \neq M'(X)$，但检错码是相同的。

【例题4.3】 用户 A 的 RSA 公钥和私钥对为 PKA 和 SKA，用户 B 的 RSA 公钥和私钥对为 PKB 和 SKB，如果用户 B 需要确定数据发送者是用户 A，而用户 A 只希望用户 B 能读取数据，用户 A 如何封装数据？如果用户 A 将发送大量数据给用户 B，如何解决发送端身份鉴别和数据加密的问题？

【解析】 如图 4.1(a)所示，为了让用户 B 能够确定数据发送者是用户 A，用户 A 需要附加数字签名 D_{SKA}(MD(P))。为了保证只有用户 B 才能读取数据，需要用用户 B 的公钥 PKB 对数据进行加密，生成密文 E_{PKB}(P)。

由于 RSA 加密过程比较复杂，不适合对大量数据进行加密，因此，当用户 A 发送大量数据时，用户 A 随机生成一个对称密钥 KEY，然后用对称密钥加密算法 DE 和对称密钥 KEY 对数据加密，生成密文 DE_{KEY}(P)。为了保证只有用户 B 才能读取数据，用用户 B 的公钥 PKB 对对称密钥 KEY 进行加密，生成数字信封 E_{PKB}(KEY)。由于只有用户 B 才

能解密出对称密钥 KEY，因此，只有用户 B 才能解密出数据，数据封装过程如图 4.1(b) 所示。

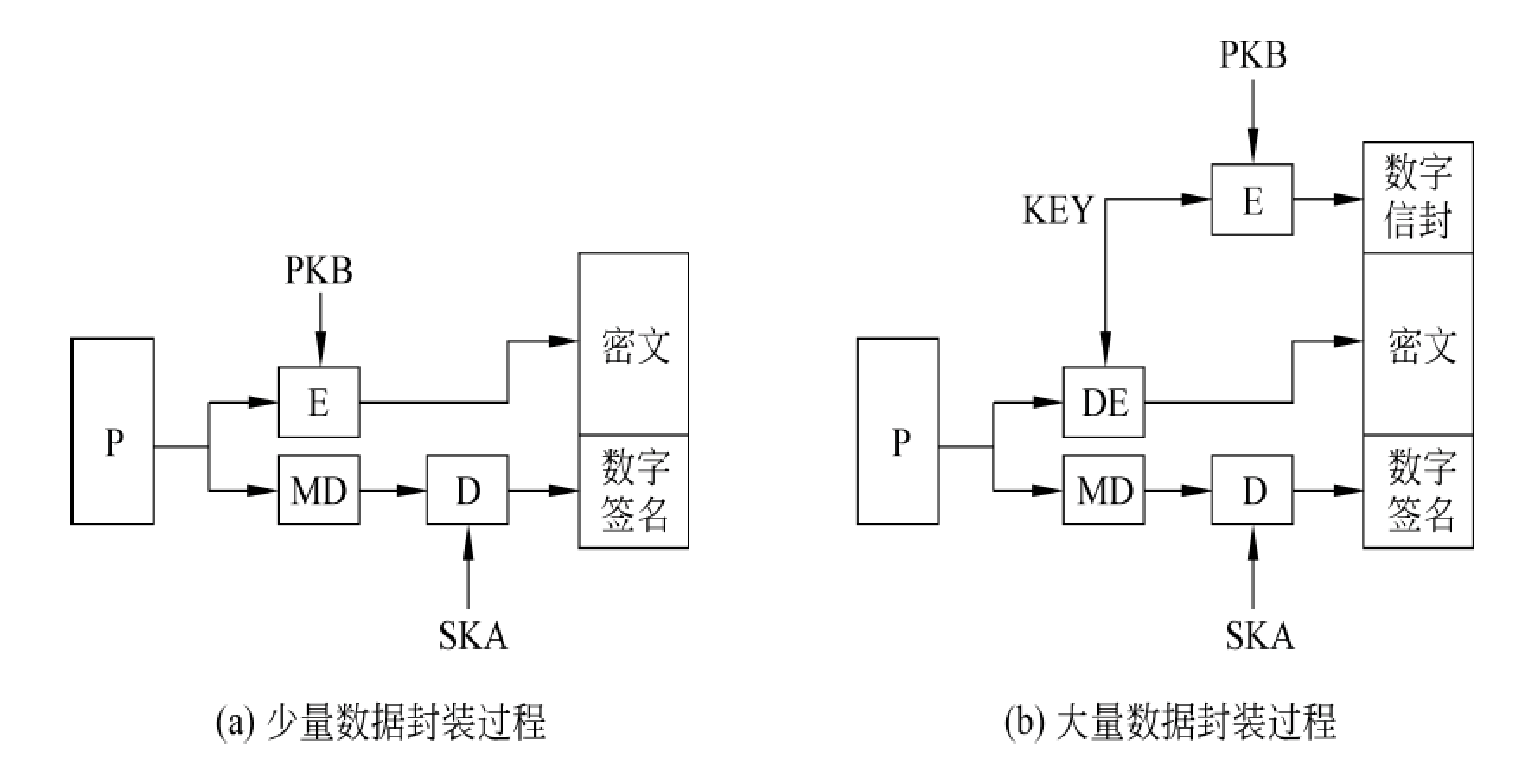


图 4.1　用户 A 封装数据过程

【例题 4.4】 如果图 4.2 中的终端实体 3 需要证明终端实体 1 与其公钥之间的绑定关系，给出终端实体 1 发送给终端实体 3 的证书链，并简述根据证书链证明终端实体 1 与其公钥之间绑定关系的过程。

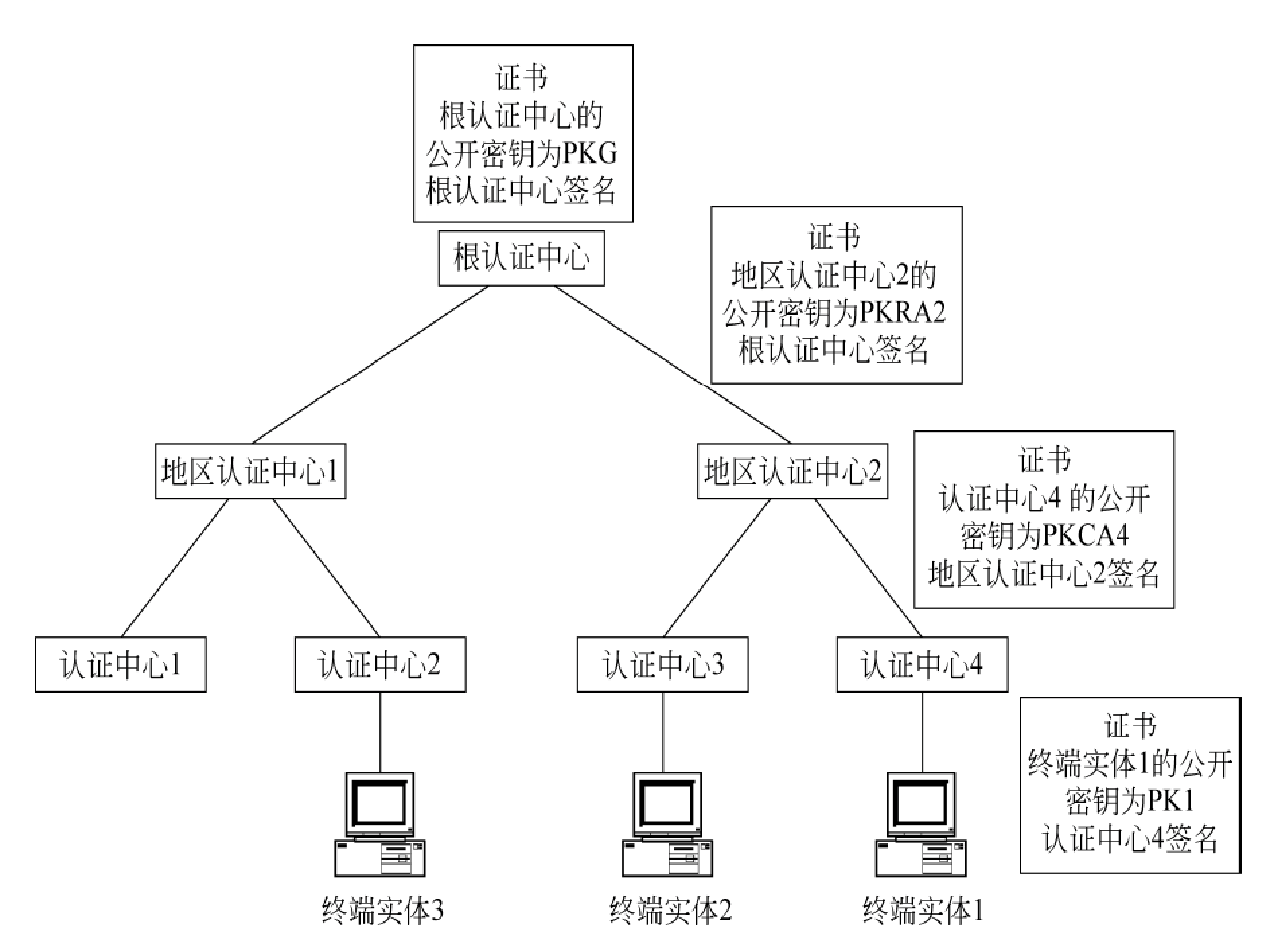


图 4.2　分层认证结构

【解析】 终端实体 1 发送的证书链如下：根认证中心＜＜地区认证中心 2＞＞，地区认证中心 2 ＜＜认证中心 4＞＞，认证中心 4＜＜终端实体 1＞＞，其中用 Y＜＜X＞＞表示由认证中心 Y 签发的用于证明用户 X 和某个公钥之间绑定关系的证书。

终端实体 3 通过有公信力的媒介获取根认证中心的公钥 PKG，同时验证根认证中心公钥 PKG 与根认证中心之间的绑定关系。

终端实体 3 通过证书“根认证中心＜＜地区认证中心 2＞＞”获取地区认证中心 2 的公钥 PKRA2，用根认证中心的公钥 PKG 验证地区认证中心 2 的公钥 PKRA2 与地区认证中心 2 之间的绑定关系。

终端实体 3 通过证书“地区认证中心 2 ＜＜认证中心 4＞＞”获取认证中心 4 的公钥 PKCA4，用地区认证中心 2 的公钥 PKRA2 验证认证中心 4 的公钥 PKCA4 与认证中心 4 之间的绑定关系。

终端实体 3 通过证书“认证中心 4＜＜终端实体 1＞＞”获取终端实体 1 的公钥 PK1，用认证中心 4 的公钥 PKCA4 验证终端实体 1 的公钥 PK1 与终端实体 1 之间的绑定关系。

【例题 4.5】 假定用户 A 和用户 B 约定采用 RSA 公开密钥加密算法和 MD5 报文摘要算法。用户 A 的公钥是 PKA、私钥是 SKA。用户 B 的公钥是 PKB、私钥是 SKB。假定用户 A 和用户 B 已经拥有对方的公钥。回答以下问题。

(1) 如果用户 A 用对称密钥加密算法加密向用户 B 发送的数据，给出用户 A 加密过程和用户 B 解密过程，用 E 表示对称密钥加密算法，用 D 表示对称密钥解密算法。

(2) 给出用户 A 对发送给用户 B 的数据实施数字签名的过程和用户 B 验证用户 A 数字签名的过程。用 RASE 表示 RSA 加密算法，用 RASD 表示 RAS 解密算法。

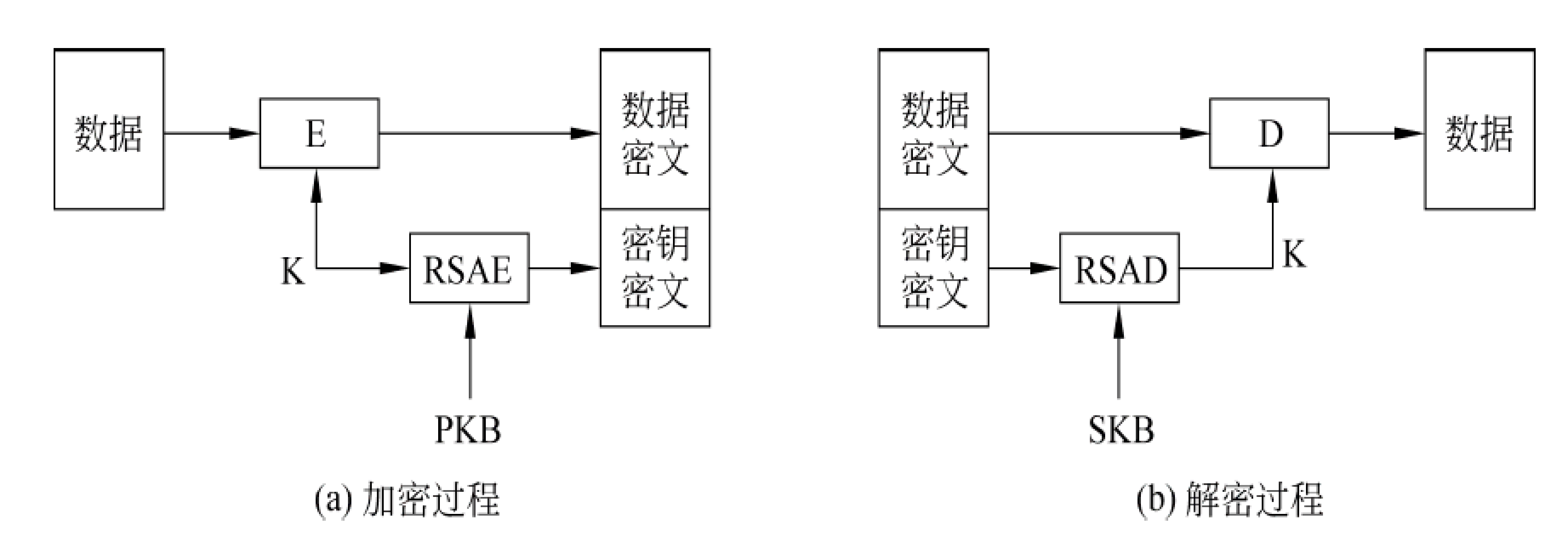
(3) 如果用户 A 用用户名用户 A 和口令 PASSA 作为用户身份标识信息，给出用户 B 鉴别用户 A 身份的过程。

(4) 如果用户 A 和用户 B 通过证书和私钥作为用户身份标识信息，给出用户 A 和用户 B 通过数字签名完成双向身份鉴别的过程。

【解析】

(1) 如图 4.3 所示，假定用户 A 发送给用户 B 的数据是 P，用户 A 随机产生对称密钥 K，用加密算法 E 和对称密钥 K 对数据 M 进行加密，得到密文 $E_K(P)$。用 RSA 加密算法 RSAE 和用户 B 的公钥 PKB 对密钥 K 进行加密，得到密文 $RSAE_{PKB}(K)$。用户 A 向用户 B 发送 $E_K(P) \| RSAE_{PKB}(K)$。

用户 B 首先用私钥 SKB 和 RSA 解密算法 RSAD 对密文 $RSAE_{PKB}(K)$ 进行解密，得到密钥 K($RSAD_{SKB}(RSAE_{PKB}(K))=K$)。然后用解密算法 D 和密钥 K 对密文 $E_K(P)$ 进行解密，得到数据 P($D_K(E_K(P))=P$)。



(a) 加密过程 (b) 解密过程

图 4.3 加密/解密过程

(2) 如图 4.4 所示，假定用户 A 发送给用户 B 的数据是 P，用户 A 生成数字签名

$RASD_{SKA}$(MD5(P))。用户 A 向用户 B 发送 P‖$RASD_{SKA}$(MD5(P))。

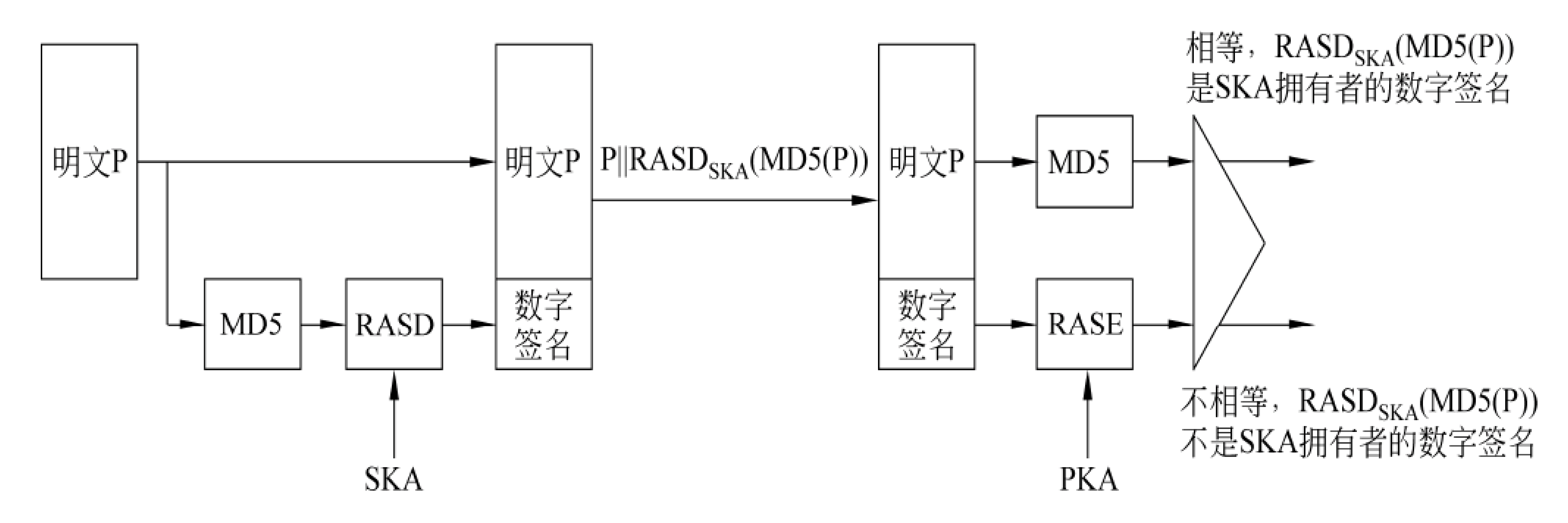


图 4.4　数字签名实现过程

用户 B 只要证明 $RASE_{PKA}$($RASD_{SKA}$(MD5(P)))=MD5(P)，即可证明 $RASD_{SKA}$(MD5(P))是用户 A 对数据 P 签署的数字签名。

(3) 如图 4.5 所示，用户 B 为了证明用户 A 知道口令 PASSA，向用户 A 发送随机数 R_B，用户 A 向用户 B 发送用户 A‖MD5(R_B‖PASSA)。只要用户 B 的计算结果 MD5(R_B‖PASSA)和用户 A 发送的 MD5(R_B‖PASSA)相等，即可证明用户 A 知道口令 PASSA。

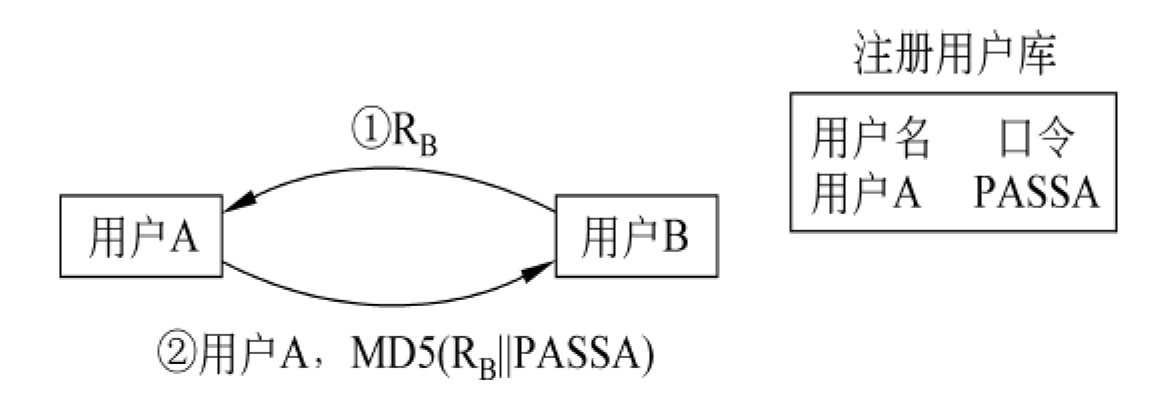


图 4.5　基于用户名和口令的单向鉴别过程

(4) 如图 4.6 所示，用户 B 为了证明用户 A 拥有私钥 SKA，向用户 A 发送随机数 R_B，用户 A 生成随机数 R_A 和数字签名 $RASD_{SKA}$(MD5(R_A‖R_B))，向用户 B 发送 R_A‖$RASD_{SKA}$(MD5(R_A‖R_B))。用户 B 只要证明 $RASE_{PKA}$($RASD_{SKA}$(MD5(R_A‖R_B)))=MD5(R_A‖R_B)，即可证明用户 A 拥有私钥 SKA。

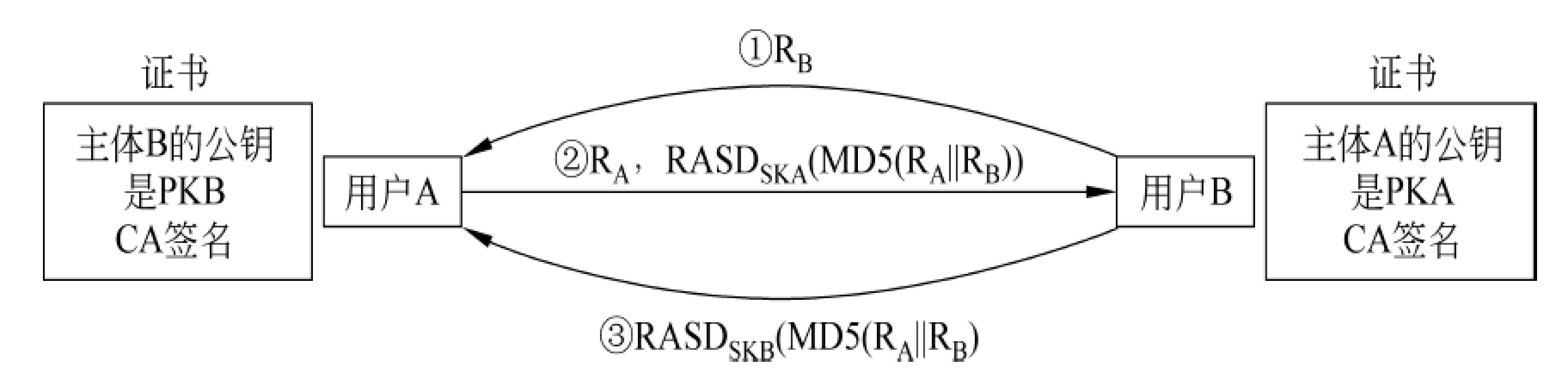


图 4.6　基于证书和私钥的双向鉴别过程

同样，用户 B 为向用户 A 证明拥有私钥 SKB，向用户 A 发送 $RASD_{SKB}$(MD5(R_A‖R_B))。用户 A 只要证明 $RASE_{PKB}$($RASD_{SKB}$(MD5(R_A‖R_B)))=MD5(R_A‖R_B)，即可证明用户 B 拥有私钥 SKB。

4.2 选择题分析

(1) 以下哪一项是检错码不能用于完整性检测的原因?( )

A. 检错码算法一般不具有抗碰撞性

B. 检错码是用于检测传输错误的附加信息

C. 好的检错码算法使检错码可以检测出尽可能多的传输错误

D. 检错码算法通常具有单向性

答案:A

【分析】 完整性检测需要能够检测出精心设计的篡改,因此,抗碰撞性是至关重要的,检错码算法一般不具备抗碰撞性。

(2) 关于报文摘要算法,以下哪一项描述是错误的?( )

A. 具有单向性

B. 具有抗碰撞性

C. 生成固定长度的报文摘要

D. 不同报文有着不同的报文摘要

答案:D

【分析】 任意长度的报文生成固定长度的报文摘要,肯定存在多个不同的报文映射到同一报文摘要的情况。抗碰撞性不是指不同报文有着不同的报文摘要,而是根据现有的计算能力,找不出跟某个已有报文不同但报文摘要相同的另一个报文。

(3) 以下哪一项表示两个不同的消息具有相同的消息摘要的现象?( )

A. 攻击　　B. 碰撞　　C. 散列　　D. 都不是

答案:B

【分析】 两个不同的消息具有相同的消息摘要的现象称为碰撞。

(4) 关于报文摘要算法,以下哪一项描述是错误的?( )

A. 报文摘要长度越大,抗碰撞性越好

B. 报文摘要长度越大,计算复杂性越高

C. 运算过程越复杂,单向性和抗碰撞性越好

D. 可以指定任意固定值作为报文摘要长度

答案:D

【分析】 报文摘要长度必须大于某个阈值才能保证报文摘要算法的抗碰撞性。

(5) 关于 MD5 报文摘要长度,以下哪一项描述是正确的?( )

A. 64　　B. 128　　C. 256　　D. 512

答案:B

【分析】 128 位报文摘要长度是综合考虑计算复杂性和抗碰撞性与单向性的结果。

(6) 关于 SHA-1 报文摘要长度,以下哪一项描述是正确的?( )

A. 128　　B. 160　　C. 256　　D. 512

答案:B

【分析】 SHA-1 报文摘要长度是 160 位，显然比 MD5 有着更好的抗碰撞性和单向性。但算法的计算复杂性也大于 MD5。

(7) 信息通过网络进行传输的过程中，存在着被篡改的风险，为了解决这一安全隐患，通常采用以下哪一项安全防护技术？(　　)

A. 加密技术　　　　B. 匿名技术

C. 消息认证技术　　　　D. 数据备份技术

答案： C

【分析】 消息认证技术也称消息鉴别技术，可以检测出消息传输过程中发生的篡改。

(8) 关于消息鉴别码，以下哪一项描述是错误的？(　　)

A. 可以直接通过消息计算得出

B. 通过密钥和消息计算得出

C. 密钥是发送端和接收端之间的共享密钥

D. 黑客无法根据篡改后的消息计算出消息鉴别码

答案： A

【分析】 消息鉴别码通常是对消息的报文摘要(也称消息摘要)进行加密运算后得到的结果，因此，无法直接通过消息计算得出。

(9) 关于消息鉴别，以下哪一项描述是错误的？(　　)

A. 对称密钥既可提供保密性又可提供消息鉴别

B. 公开密钥既可提供消息鉴别又可提供数字签名

C. 消息鉴别码是一个利用密钥生成的、附加在消息之后的、固定长度的数据块

D. 消息鉴别码既可提供消息鉴别又可提供保密性

答案： D

【分析】 消息鉴别码的主要作用有两个：一是用于确定消息源端；二是用于对消息进行完整性检测。消息鉴别码本身无法保证消息的保密性。

(10) 关于消息鉴别，以下哪一项描述是错误的？(　　)

A. 传统密码只能提供保密性，不能用于消息鉴别

B. 公钥密码既能提供保密性，又能用于消息鉴别

C. 消息鉴别是验证接收到的消息确实来自真正的发送方，并且未被篡改的过程

D. 哈希函数(报文摘要算法)的输入是可变大小的消息，输出是固定大小的哈希值(报文摘要)

答案： A

【分析】 传统密码是指对称密钥加密算法，对称密钥加密算法可以用于消息鉴别。

(11) 关于 HMAC-SHA-1-160，以下哪一项描述是错误的？(　　)

A. 先对报文进行 SHA-1 运算，再对 SHA-1 报文摘要进行加密运算

B. HMAC 的长度是 160 位

C. 密钥的长度一般要求大于 160 位

D. HMAC-SHA-1-160 的安全性基于密钥的安全性

答案：A

【分析】 HMAC-SHA-1-160 的输入是密钥和报文串接后的结果，输出是 160 位 SHA-1 报文摘要。

(12) 关于完整性检测，以下哪一项描述是正确的？(　　)

A. 黑客无法篡改报文 P

B. 黑客无法篡改附加信息 C

C. 黑客无法同时篡改报文 P 和附加信息 C

D. 黑客无法通过同时篡改报文 P 和附加信息 C，且使篡改后的报文 P 和附加信息 C 能够保持一致性

答案：D

【分析】 无法通过同时篡改报文 P 和附加信息 C，且使篡改后的报文 P 和附加信息 C 能够保持一致性是检测出精心设计的篡改的前提。

(13) 关于消息鉴别，以下哪一项描述是错误的？(　　)

A. 接收端确认是发送端 X 发送了消息 M

B. 只有接收端和发送端知道共享密钥 K

C. 只有发送端能够根据报文 M 生成 $E_K(MD(M))$

D. 发送端和接收端都能够根据报文 M 生成 $E_K(MD(M))$

答案：C

【分析】 发送端和接收端都能够根据任意报文 M，生成 $E_K(MD(M))$。因此，报文 M 和 $E_K(MD(M))$ 只能用于接收端确认是具有共享密钥 K 的发送端发送了报文 M。

(14) 以下哪一项是银行只存储密码的报文摘要的原因？(　　)

A. 无法根据密码的报文摘要导出密码

B. 计算密码的报文摘要比加密密码简单

C. 可以通过密码的报文摘要还原出密码

D. 通过密码的报文摘要还原出密码的过程比解密密码简单

答案：A

【分析】 用户一旦设定密码后，则密码对银行是不可见的，因此，银行员工无法同时泄露账号和密码，以此保证账号的安全。

(15) 以下哪一项是用 RSA 生成数字签名的先决条件？(　　)

A. 公钥和私钥一一对应

B. 私钥只有签名者自己知道

C. 由权威机构证明公钥和签名者之间的关联

D. 以上全部

答案：D

【分析】 A、B 和 C 三个选项保证数字签名的唯一性和第三方的可证明性，这两项特性都是数字签名的先决条件。

(16) 数字签名中对报文进行报文摘要运算是为了确定数字签名与报文之间的以下哪一项？(　　)

A. 关联性　　B. 保密性　　C. 可证明性　　D. 以上全部

答案：A

【分析】 由于报文摘要算法的抗碰撞性，使报文摘要和报文之间的关联性得到保证。

(17) 关于数字签名，以下哪一项描述是正确的？(　　)

A. 数字签名是在所传输的数据后附加的一段和传输数据毫无关系的数字信息

B. 数字签名能够解决数据的加密传输

C. 数字签名一般采用对称加密机制

D. 数字签名能够解决篡改、伪造等安全性问题

答案：D

【分析】 数字签名本身可以作为消息鉴别码，用于消息的完整性检测。

(18) 甲收到一份来自乙的电子订单，在将订单中的货物送达到乙时，乙否认自己曾经发送过这份订单，为了消除这种纷争，采用的安全技术是(　　)。

A. 数字签名技术　　B. 数字证书

C. 消息认证码　　D. 身份认证技术

答案：A

【分析】 数字签名技术使发送端无法否认曾经发送过的电子订单。

(19) 数字签名最常见的实现方法是建立在以下哪一对组合之上的？(　　)

A. 公钥密码体制和对称密码体制

B. 对称密码体制和报文摘要算法

C. 公钥密码体制和报文摘要算法

D. 公证系统和报文摘要算法

答案：C

【分析】 最常见的数字签名是建立在公钥密码体制和报文摘要算法上的。

(20) 关于数字签名，以下哪一项描述是错误的？(　　)

A. 只有发送端能够生成数字签名

B. 接收端能够验证数字签名

C. 数字签名与特定报文关联

D. 任何指定报文只能生成一个数字签名

答案：D

【分析】 数字签名的唯一性指的是只能由私钥的拥有者生成数字签名。对于指定报文 P，$D_{SK}(MD(P))$ 和 $D_{SK}(P)$ 都是针对报文 P 的数字签名。其中 SK 是私钥，D 是解密算法，MD 是报文摘要算法。

(21) 以下选项中，哪一项不是报文摘要算法的应用？(　　)

A. 消息鉴别　　B. 数据加密　　C. 数字签名　　D. 口令保护

答案：B

【分析】 报文摘要算法不能用于数据加密。

(22) 假定 D 是 RSA 解密算法，E 是 RSA 加密算法，SK 是私钥，PK 是 SK 对应的公

钥。关于D_{SK}(MD(P))作为数字签名的原因,以下哪一项描述是错误的?(　　)

A. 私钥 SK 由发送者唯一拥有

B. 只能根据报文 P 生成 MD(P)

C. 通过$E_{PK}(D_{SK}(MD(P)))$=MD(P)验证数字签名

D. 公钥 PK 是随便获取的

答案:D

【分析】 公钥 PK 与私钥 SK 拥有者之间的绑定关系必须得到权威机构证明,因此,通常用证书的方式由权威机构发布公钥 PK 及公钥 PK 与私钥 SK 拥有者之间的绑定关系。

(23) 以下关于数字证书的叙述中,哪一项是错误的?(　　)

A. 证书通常由 CA 颁发

B. 证书携带持有者的公开密钥

C. 证书的真实性可以通过验证证书的签名获知

D. 证书通常携带 CA 的公开密钥

答案:D

【分析】 证书中携带证书持有者的公开密钥和颁发证书的 CA 的数字签名,但不会携带 CA 的公开密钥。

(24) 以下信息中,哪一项不包含在数字证书中?(　　)

A. 用户身份标识　　B. 用户的公钥

C. 用户的私钥　　D. CA 的数字签名

答案:C

【分析】 用户的私钥只能由用户掌握,不能出现在证书中。

(25) 以下哪一项不是数字签名的特性?(　　)

A. 唯一性　　B. 与特定报文关联性

C. 可证明性　　D. 保密性

答案:D

【分析】 数字签名可以保证所签名报文的完整性和不可抵赖性,但不保证所签名报文的保密性。

(26) 以下哪一项不属于 PKI 的功能?(　　)

A. 用证书证明公钥与用户标识信息之间的关联

B. 管理证书

C. 生成公钥和私钥对

D. 分配共享密钥

答案:D

【分析】 PKI 是证书和公钥管理平台。

(27) 以下哪一项不是验证证书时需要验证的内容?(　　)

A. 验证有效性,即证书是否在证书的有效使用期之内

B. 验证可用性,即证书是否已经废除

C. 验证真实性,即证书是否由信任的 CA 签发

D. 验证保密性,即证书是否由 CA 进行了加密

答案: D

【分析】 证书内容是公开的,不需要加密。

(28) 在 PKI 中,不属于 CA 的任务是(　　)。

A. 证书的颁发　　B. 证书的审批

C. 证书的备份　　D. 证书的加密

答案: D

【分析】 CA 不对证书进行加密。

(29) 关于认证中心和证书,以下哪一项描述是错误的?(　　)

A. 认证中心颁发证书

B. 证书有认证中心的数字签名

C. 认证中心与公钥之间的绑定关系由上一级认证中心证明

D. 证书可以伪造

答案: D

【分析】 认证中心的数字签名有两个作用:一是用于对证书进行完整性检测;二是证明该证书确实由认证中心颁发。因此,认证中心颁发的证书是不能伪造的。

(30) 关于层次结构中的根认证中心,以下哪一项描述是错误的?(　　)

A. 公钥通过有公信力的媒体发布

B. 证明公钥与根认证中心之间绑定关系的证书由根认证中心的私钥签名

C. 根认证中心可以作为所有属于该层次结构的实体的信任锚

D. 证明公钥与根认证中心之间绑定关系的证书无须验证

答案: D

【分析】 由于证明公钥与根认证中心之间绑定关系的证书由根认证中心的私钥签名,因此,需要根认证中心的公钥验证证书的真伪。但根认证中心的公钥是通过有公信力的媒体发布的,不是由证书给出的。

(31) 关于实体 X 和实体 Y 的共同信任锚,以下哪一项描述是错误的?(　　)

A. 实体 X 和实体 Y 都已经验证用于证明信任锚的公钥与信任锚之间绑定关系的证书

B. 实体 X 和实体 Y 的认证路径都是从信任锚开始的

C. 实体 X 和实体 Y 的认证路径是相同的

D. 根据实体 X 和实体 Y 的认证路径,可以构建以信任锚为根认证中心包含实体 X 和实体 Y 的层次结构

答案: C

【分析】 除了证明实体 X 和实体 Y 与其公钥之间绑定关系的证书由同一个认证中心颁发的情况外,实体 X 和实体 Y 的认证路径是不同的。

4.3 名词解释

(1) 报文摘要

标识某个任意长度报文的有限位数信息,而且这种标识信息就如同报文的指纹一样,具有确认性和唯一性。

(2) 报文摘要算法

一种将任意长度的报文转换成报文摘要的算法,且该算法具有单向性和抗碰撞性。

(3) 单向性

只能根据报文 X 求出 MD(X),从计算可行性讲,无法根据标识信息 h 得出报文 X,且使 MD(X)=h。

(4) 抗碰撞性

从计算可行性而言,对于任意报文 X,无法找出另一个报文 Y,X≠Y,但 MD(X)=MD(Y)。

(5) MD5

一种将任意长度的报文转换成 128 位的报文摘要的算法。

(6) SHA-1

一种将任意长度的报文转换成 160 位的报文摘要的算法。

(7) 消息鉴别码

根据需要进行完整性检测的消息计算得出的、用于实现消息完整性检测的附加信息。

(8) 消息鉴别

验证消息 M 确实是 X 发送的过程。

(9) 数字签名

某个报文的附加信息,该附加信息既能够证明签名者的真实性,也能够证明签名者对该报文的确认。

(10) 认证中心

具有公信力的权威机构,颁发用于证明公钥与某个实体之间绑定关系的证书。

(11) 证书

由认证中心数字签名的、用于证明公钥与某个实体之间绑定关系的文书。

(12) PKI

一种用于管理、控制证书全过程的基础设施,包括证书的生成、更新、撤销和交叉认证机制等。

(13) 源端鉴别

一种通过在报文中嵌入发送端标识信息,使接收端能够验证报文发送端的技术。

第 5 章 接入控制和访问控制

5.1 例题解析

5.1.1 简答题解析

【例题 5.1】 简述接入控制设备的作用。

【解析】 接入控制设备的作用主要有以下两个：一是作为普通路由器实现接入网络与 Internet 的互连；二是完成对用户终端的接入控制过程，主要功能包括鉴别接入用户身份、动态分配 IP 地址、建立用于指明通往用户终端的传输路径的路由项。

【例题 5.2】 简述接入控制和身份鉴别之间的关系。

【解析】 接入控制是只允许主体 X 使用的终端接入网络的控制过程。身份鉴别是确定主体 X 身份的过程。通常在身份鉴别过程中建立主体 X 与某个标识信息之间的绑定关系，随后，通过判别是否携带与主体 X 绑定的标识信息判定是否是主体 X 使用的终端发送的信息。该标识信息可以是终端的 MAC 地址或 IP 地址，这种情况下，只有源 MAC 地址是与主体 A 绑定的 MAC 地址的 MAC 帧，或者源 IP 地址是与主体 A 绑定的 IP 地址的 IP 分组，才是主体 X 使用的终端发送的 MAC 帧或 IP 分组。

【例题 5.3】 简述鉴别者和鉴别服务器需要将 EAP 报文封装成 RADIUS 消息，而不是直接封装成 IP 分组的原因。

【解析】 RADIUS 的主要功能有以下两个：一是实现鉴别者与鉴别服务器之间的双向身份鉴别；二是实现敏感信息鉴别者与鉴别服务器之间的安全传输过程。IP 分组经过互连网传输的过程中，既无法对发送端和接收端的身份进行双向鉴别，也无法实现 IP 分组发送端和接收端之间的安全传输。因此，不能直接将 EAP 报文封装成 IP 分组，然后通过互连网实现 IP 分组鉴别者和鉴别服务器之间的传输过程。

【例题 5.4】 简述 Kerberos 用户和鉴别服务器之间基于共享密钥的身份鉴别过程和防中间人攻击机制。

【解析】 由于只有某个授权用户和鉴别服务器才能够知道该授权用户的口令，而共享密钥 K_C是通过该授权用户的口令导出的，因此，只要双方能够导出相同的共享密钥 K_C，用户和鉴别服务器的身份就能得到证实。

如果黑客能够截获用户发送给鉴别服务器的身份鉴别请求，并将用户名由 ID_C改为 ID_H，将封装身份鉴别请求的 IP 分组的源 IP 地址由 AD_C改为 AD_H。鉴别服务器生成的票据中的用户名和终端地址也将改为 ID_H和 AD_H。但由于黑客无法导出共享密钥 K_C，因

而无法获得鉴别服务器生成的用户与票据授权服务器之间的共享密钥 $K_{C,TGS}$，因此，无法生成用共享密钥 $K_{C,TGS}$ 加密 ID_H 后得到的鉴别信息，从而无法让票据授权服务器确认鉴别服务器已经完成对黑客的身份鉴别过程。

【例题 5.5】 简述资源访问控制原理及过程。

【解析】 配置授权用户身份标识信息；为每一个授权用户分配资源访问权限；一旦用户提出资源访问请求，首先鉴别该用户身份，鉴别用户身份的过程就是确定该用户提供的身份标识信息是否和配置的某个授权用户的身份标识信息相同的过程；确定用户提出的资源访问请求是否符合分配该用户的资源访问权限；在确定该用户为授权用户且具有资源访问请求中要求的资源访问权限后，完成资源访问过程。

5.1.2 设计题解析

【例题 5.6】 如果采用基于证书和私钥的身份鉴别机制，且鉴别身份时使用的私钥和数字签名时使用的私钥相同，会有什么后果？

【解析】 如果主体 A 鉴别身份时使用的私钥和数字签名时使用的私钥相同，主体 B 可以利用身份鉴别过程生成主体 A 对消息 P 的数字签名。如图 5.1 所示，主体 B 生成消息 P，并计算出消息 P 的报文摘要 MD(P)。然后主体 B 发起对主体 A 的身份鉴别过程，向主体 A 发送 MD(P)，主体 A 为了证明拥有私钥 SKA，生成并向主体 B 发送 D_{SKA}(MD(P))，其中 D 是 RSA 解密算法。主体 B 根据消息 P 和 D_{SKA}(MD(P))可以证明主体 A 向主体 B 发送了消息 P，且对消息 P 进行数字签名。

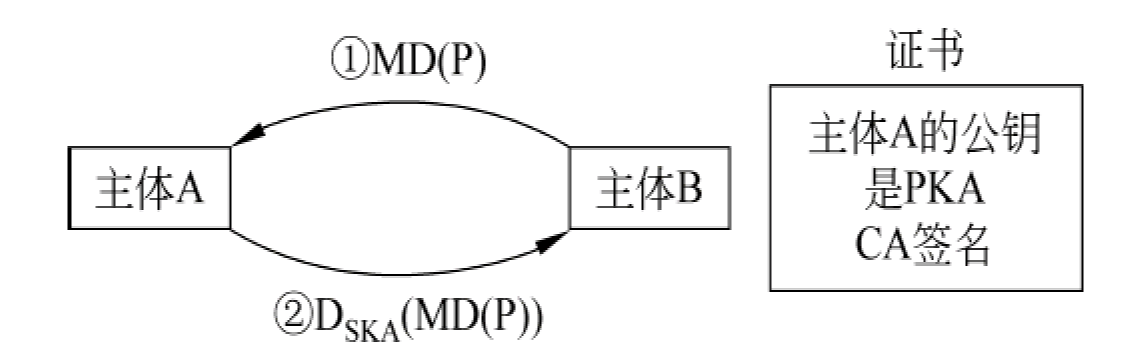


图 5.1 主体 B 利用身份鉴别过程获取主体 A 的数字签名

【例题 5.7】 假定基于共享密钥的接入控制过程如图 5.2(a)所示，终端 A 只要能够向交换机证明自己知道共享密钥 K，交换机则允许终端 A 接入，即允许转发以 MAC A 为源或目的 MAC 地址的 MAC 帧，但如图 5.2(a)所示的基于共享密钥的接入控制过程容易招致如图 5.2(b)所示的中间人攻击过程。如果黑客终端能够截获终端 A 与交换机之间传输的 MAC 帧，黑客终端可以将终端 A 发送的 MAC 帧篡改为黑客终端发送的 MAC 帧，并将交换机发送给它的随机数转发给终端 A。最终结果是导致交换机允许不知道共享密钥的黑客终端接入。修正如图 5.2(a)所示的基于共享密钥的接入控制过程，使黑客

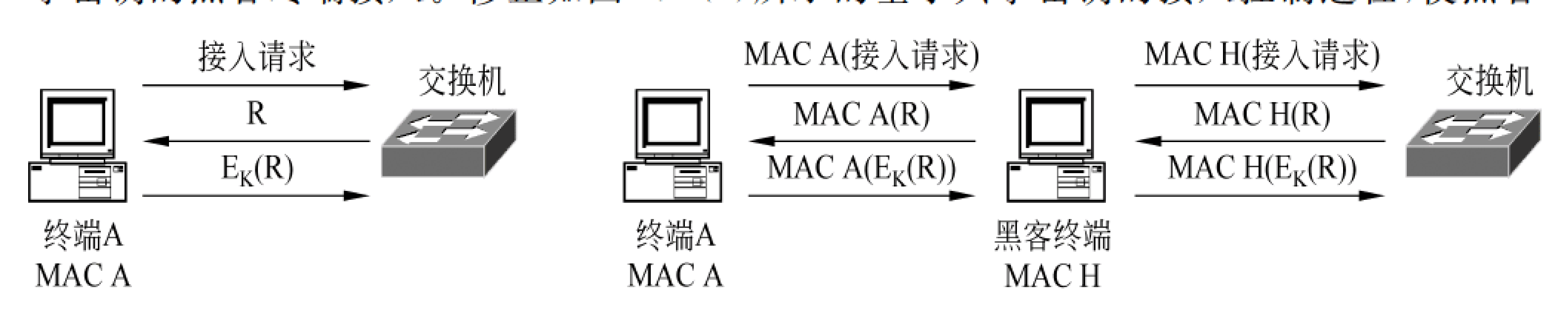


图 5.2 基于共享密钥的接入控制过程

终端无法通过如图 5.2(b)所示的中间人攻击过程接入交换机。

【解析】 改进后的基于共享密钥的接入控制过程如图 5.3 所示，终端 A 接收到交换机发送的随机数 R 后，将随机数 R 和自己的 MAC 地址 MAC A 串接在一起，用共享密钥 K 对串接结果进行加密，生成密文 $E_K(R \| MAC\ A)$，然后把密文发送给交换机。交换机用共享密钥解密密文后，得到 R‖MAC A，根据随机数 R，确定终端 A 具有共享密钥 K，允许转发以 MAC A 为源或目的 MAC 地址的 MAC 帧。

【例题 5.8】 假定用户 A 和用户 B 有着共享密钥 KAB，用户 A 和用户 B 通信时，确定双方身份的过程如图 5.4 所示。假定用户 C 能够截获用户 A 发送给用户 B 的鉴别消息，给出用户 C 让用户 A 误认为是用户 B 的过程，并给出如图 5.6 所示的确定双方身份过程的改进版。

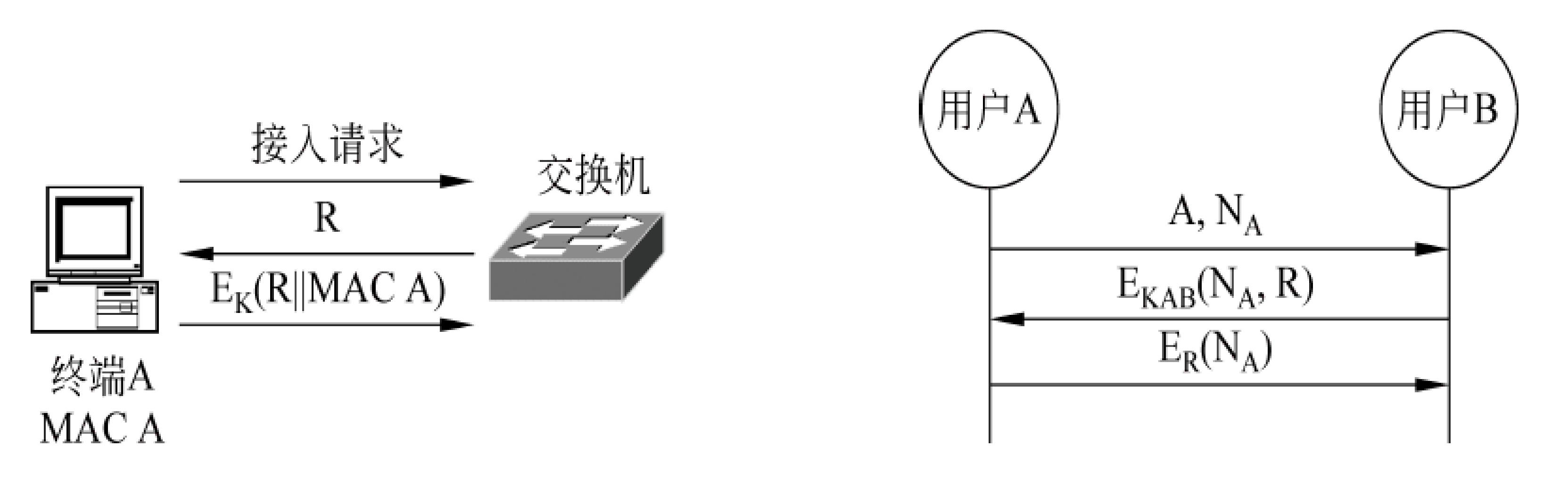


图 5.3　改进后的基于共享密钥的接入控制过程

图 5.4　相互确认通信另一方身份的过程

【解析】 当用户 C 截获到用户 A 发送给用户 B 的鉴别消息(A, N_A)时，冒充用户 B 向用户 A 发送鉴别消息(B, N_A)，如图 5.5 所示。当用户 A 接收到鉴别消息(B, N_A)时，用用户 A 和用户 B 之间的共享密钥 KAB 加密 N_A 和用户 A 随机生成的会话密钥 R，然后将密文 $E_{KAB}(N_A, R)$发送给用户 B。用户 C 截获密文 $E_{KAB}(N_A, R)$后，将密文 $E_{KAB}(N_A, R)$发送给用户 A，用户 A 误认为密文 $E_{KAB}(N_A, R)$是用户 B 针对鉴别消息(A, N_A)发送的响应消息，确认用户 C 是用户 B。

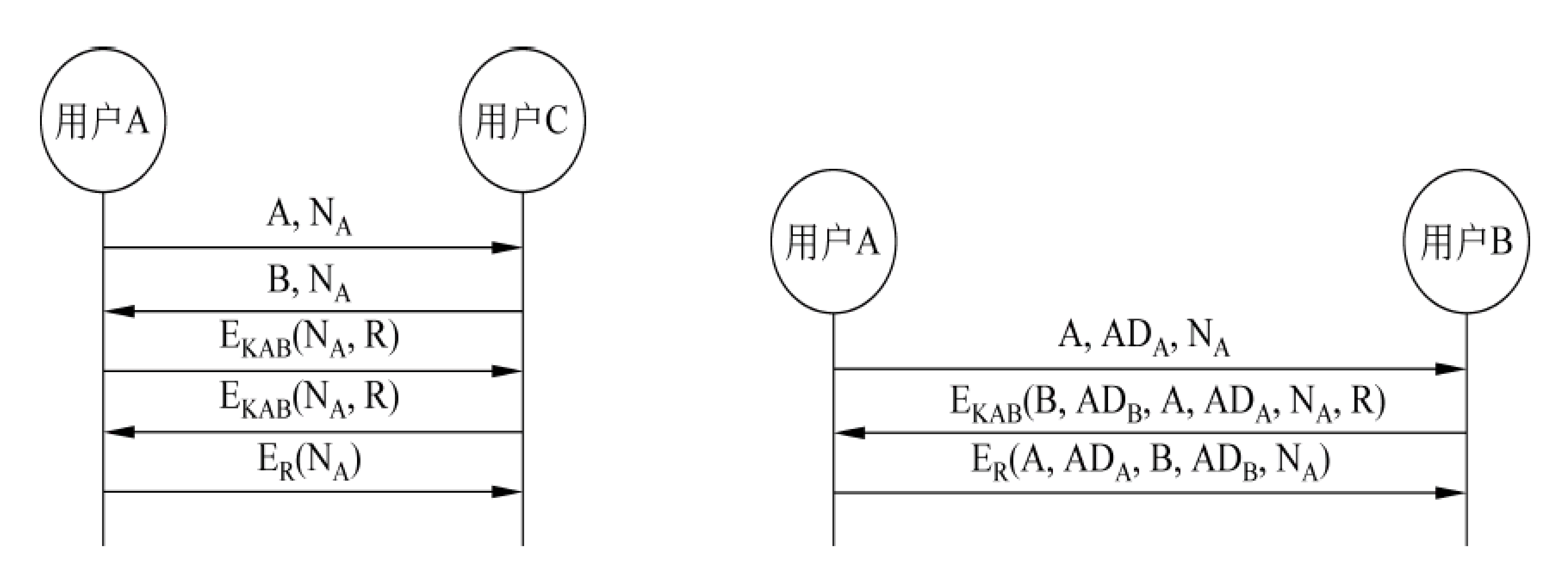


图 5.5　用户 C 冒充用户 B 的过程

图 5.6　改进后的相互确认对方身份的过程

假定用户 A 终端的 IP 地址是 AD_A，用户 B 终端的 IP 地址是 AD_B，改进后的相互确认对方身份的过程如图 5.6 所示，用户 A 发送给用户 B 的鉴别消息中包含用户 A 的 IP 地址 AD_A，用户 B 发送的针对鉴别消息(A, AD_A, N_A)的响应消息是：用用户 A 和用户 B 之间的共享密钥 KAB 对用户 B 的标识符 B、用户 B 终端的 IP 地址 AD_B、用户 A 的标识符 A、用户 A 终端的 IP 地址 AD_A、随机数 N_A 和用户 B 随机生成的会话密钥 R 加密后生

成的密文 $E_{KAB}(B,AD_B,A,AD_A,N_A,R)$。用户 A 接收到密文 $E_{KAB}(B,AD_B,A,AD_A,N_A,R)$后，如果用用户 A 和用户 B 之间的共享密钥 KAB 解密后得到用户 A 的标识符 A、用户 A 终端的 IP 地址 AD_A 和随机数 N_A，且解密后得到的用户 B 终端的 IP 地址 AD_B 与封装密文的 IP 分组的源 IP 地址相同，用户 B 的身份得到证实。然后，用解密后得到的会话密钥 R 对用户 A 的标识符 A、用户 A 终端的 IP 地址 AD_A、用户 B 的标识符 B、用户 B 终端的 IP 地址 AD_B 和随机数 N_A 加密，生成密文 $E_R(B,AD_B,A,AD_A,N_A)$，将密文 $E_R(B,AD_B,A,AD_A,N_A)$发送给用户 B。用户 B 接收到密文 $E_R(B,AD_B,A,AD_A,N_A)$后，如果用会话密钥 R 解密后得到用户 B 的标识符 B、用户 B 终端的 IP 地址 AD_B 和随机数 N_A，且解密后得到的用户 A 终端的 IP 地址 AD_A 与封装密文的 IP 分组的源 IP 地址相同，用户 A 的身份得到证实。

【例题 5.9】 假定用户 B 鉴别用户 A 身份的过程如图 5.7 所示，其中 PKA 是用户 A 的公钥，A 和 B 是用户 A 和用户 B 的标识符，N_B 是用户 B 选择的随机数。请回答以下问题。

(1) 身份鉴别和加密的区别。

(2) 简述 N_B 的选择原则和作用。

(3) 简述用户 A 回送 $MD(N_B)$的理由。

(4) 图 5.7 所示的用户 B 鉴别用户 A 身份的过程存在哪些缺陷，请给出解决思路。

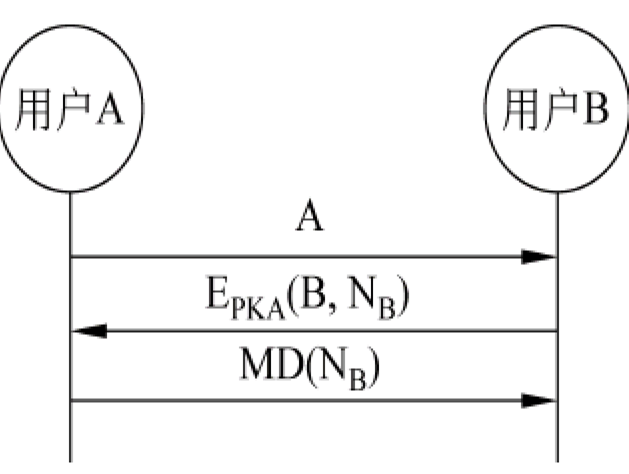


图 5.7 用户 B 鉴别用户 A 身份的过程

【解析】

(1) 身份鉴别是验证主体的真实身份与其所声称的身份是否符合的过程，主体可以是用户、进程和主机等。验证主体 X 的身份需要做到以下两点：一是接收到只能由主体 X 生成的信息；二是确认接收到的信息是主体 X 发送的。加密是保证只允许授权访问的主体能够访问到某个信息的过程。当授权访问某个信息的主体大于 2 时，主体无法通过访问到该信息证明自己的身份。

(2) N_B 是随机数，具有以下两个特征：一是不会重复出现；二是无法预测。保证每一次身份鉴别时，用户 B 发送给用户 A 的 N_B 是不同的，且用户 A 无法预测下一次身份鉴别时用户 B 发送的 N_B，以此避免重放攻击。

(3) 报文摘要算法具有单向性和抗碰撞性，因此，用户 A 回送 $MD(N_B)$，既可以让用户 B 确认用户 A 获得 N_B，又保证其他主体无法截获 N_B。

(4) 虽然 $MD(N_B)$只能由用户 A 生成，但用户 B 接收到的 $MD(N_B)$可能是其他主体发送的。假如用户 C 能够截获用户 A 发送的 $MD(N_B)$，并将截获的 $MD(N_B)$转发给用户 B，使用户 B 将用户 C 误认为用户 A。

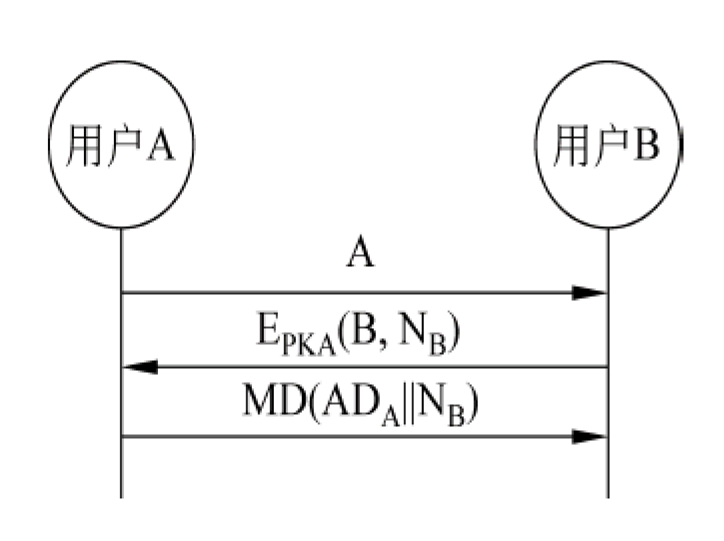


图 5.8 改进后的用户 B 鉴别用户 A 身份的过程

改进后的用户 B 鉴别用户 A 身份的过程如图 5.8 所示，用户 A 回送给用户 B 的是 $MD(AD_A \| N_B)$，其中 AD_A 是用户 A 使用的终端的 IP 地址。当用户 B 接收到封装 $MD(AD_A \| N_B)$的 IP 分组时，先将该 IP 分组的源 IP 地址和随机数 N_B 串接，并对串接结果计算报文摘要，

然后将用户 B 计算出的报文摘要与用户 A 发送的 MD($AD_A \| N_B$)进行比较，如果相等，则表明该 IP 分组确实是用户 A 所发的。

5.2　选择题分析

(1) 关于网络环境下的身份鉴别过程，以下哪一项描述是正确的？(　　)

A. 主体提供类似身份证的物理证件

B. 主体提供指纹

C. 主体提供视网膜

D. 主体提供能够证明其身份，且可以通过网络传输的主体身份标识信息

答案：D

【分析】 在网络环境下，主体和鉴别者相距甚远，无法确定经过网络传输的身份证、指纹、视网膜等扫描件与主体之间的绑定关系。

(2) 以下哪一项不是网络环境下的主体身份标识信息？(　　)

A. 密钥　　B. 用户名和口令　　C. 证书和私钥　　D. 身份证号码

答案：D

【分析】 主体身份标识信息是指可以证明主体身份的信息，鉴别者不能根据示证者能够提供 X 的身份证号码就确定示证者是 X。

(3) 对于密钥是主体身份标识信息的情况，以下哪一项描述是正确的？(　　)

A. 只有主体知道密钥

B. 只有示证者和鉴别者知道密钥

C. 主体通过向鉴别者发送密钥证明自己知道密钥

D. 只有鉴别者知道密钥

答案：B

【分析】 由于密钥只有示证者和鉴别者知道，且示证者能够向鉴别者证明自己知道密钥，示证者的身份可以因此得到证明。

(4) 对于用户名和口令是主体身份标识信息的情况，以下哪一项描述是正确的？(　　)

A. 只有主体知道用户名和口令

B. 只有示证者和鉴别者知道用户名和口令

C. 主体通过向鉴别者发送 MD(口令)证明自己知道口令

D. 只有鉴别者知道用户名和口令

答案：B

【分析】 一是不同的用户有着不同的用户名，二是每一个用户名对应一个口令。由于某对用户名和口令只有示证者和鉴别者知道，且示证者能够向鉴别者证明自己知道该对用户名和口令，示证者的身份可以因此得到证明。主体既需要向鉴别者发送用户名和口令，也不能简单地用口令的报文摘要(MD(口令))隐藏口令。

(5) 对于证书和私钥是主体身份标识信息的情况，以下哪一项描述是错误的？(　　)

A. 证书证明私钥对应的公钥与主体之间的绑定关系

B. 公钥与私钥一一对应

C. 鉴别者可以通过公钥证明主体知道私钥

D. 只有示证者和鉴别者知道私钥

答案：D

【分析】 只有主体知道私钥，鉴别者一是通过证书获取私钥对应的公钥，证明私钥对应的公钥与主体之间的绑定关系，二是通过公钥证明主体知道私钥。

(6) 如果终端已经接入 Internet，以下哪一项描述是错误的？(　　)

A. 已经建立终端与接入控制设备之间的传输路径

B. 已经为终端分配 IP 地址

C. 接入控制设备已经创建将分配给终端的 IP 地址和终端与接入控制设备之间的传输路径绑定在一起的路由项

D. 终端发送的信息中包含注册用户标识信息

答案：D

【分析】 在身份鉴别过程中，使用终端的用户需要证明自己是注册用户。一旦完成身份鉴别过程，用分配给终端的 IP 地址和已经建立的该终端与接入控制设备之间的传输路径唯一标识该注册用户使用的终端发送的数据。

(7) 以下哪一项是实现接入控制的前提？(　　)

A. 建立允许接入的授权用户的身份标识信息列表

B. 互连接入网络和 Internet 的路由器具有接入控制功能

C. 鉴别协议能够实现用户身份鉴别

D. 以上全是

答案：D

【分析】 A 和 C 选项是实现身份鉴别必需的，B 选项是接入网络结构所要求的。

(8) 对于具有 802.1X 接入控制功能的设备，以下哪一项描述是最贴切的？(　　)

A. 必须是路由器　　B. 必须是交换机

C. 可以是交换机　　D. 没有交换和路由功能的设备

答案：C

【分析】 802.1X 是以太网端口接入控制协议，具有以太网端口的设备都可具有 802.1X 接入控制功能。

(9) 对于具有 PPP 接入控制功能的设备，以下哪一项描述是最贴切的？(　　)

A. 必须是路由器　　B. 必须是交换机

C. 可以是交换机　　D. 没有交换和路由功能的设备

答案：A

【分析】 具有 PPP 接入控制功能的设备同时需要具有实现接入网络和 Internet 互连的功能。

(10) 关于接入控制设备，以下哪一项描述是错误的？(　　)

A. 是互连接入网络和 Internet 的路由器

B. 具有鉴别接入用户身份的功能

C. 具有为接入终端分配 IP 地址的功能

D. 具有发起建立与接入终端之间的传输路径的功能

答案：D

【分析】 通常由接入终端发起建立接入终端与接入控制设备之间的传输路径。

(11) 以下哪一项是接入控制的核心任务？(　　)

A. 为终端动态分配 IP 地址

B. 建立接入终端与接入控制设备之间的传输路径

C. 动态创建指明通往接入终端的传输路径的路由项

D. 鉴别启动接入终端接入 Internet 过程的用户的身份

答案：D

【分析】 接入控制的目的是只允许注册用户接入 Internet。

(12) 关于 PPP，以下哪一项描述是最贴切的？(　　)

A. PPP 是控制接入控制过程的协议

B. PPP 是鉴别用户身份的协议

C. PPP 是为终端动态分配 IP 地址的协议

D. PPP 是动态建立用于指明通往接入终端的传输路径的路由项的协议

答案：A

【分析】 PPP 只是一种控制接入控制过程的协议。其他选项的功能是在接入控制过程中由其他协议协同完成的功能。

(13) 以下哪一项功能与 PPP 作为接入控制协议无关？(　　)

A. 建立 PPP 链路时协商鉴别协议和网络控制协议

B. PPP 帧作为鉴别协议对应的协议数据单元的载体

C. PPP 帧作为 IP 控制协议对应的协议数据单元的载体

D. 实现 PPP 帧检错

答案：D

【分析】 D 选项的功能是链路层协议应该具备的功能，不是因为实现接入控制过程而增加的功能。

(14) 关于 PPP，以下哪一项描述是错误的？(　　)

A. 基于点对点信道的链路层协议

B. PSTN 作为接入网络时的接入控制协议

C. 通过 PPP over X 技术实现 PPP 帧经过多种不同类型的分组交换路径的传输过程

D. 通用的链路层协议

答案：D

【分析】 链路层协议与传输网络相关，没有适用于所有传输网络的通用链路层协议。

(15) 以下哪一项不是 PPP 链路建立过程完成的功能？(　　)

A. 两端协商与 PPP 帧传输过程相关的参数

B. 两端协商身份鉴别协议

C. 两端协商网络控制协议

D. 两端协商终端 IP 地址

答案：D

【分析】 D 选项是网络层协议配置过程完成的功能。

(16) 以下哪一种情况不是导致从身份鉴别阶段进入 PPP 链路终止阶段的原因？(　　)

A. 一端发起物理链路释放过程　　B. 物理链路上检测不到载波信号

C. 用户不是注册用户　　D. IP 地址池耗尽

答案：D

【分析】 身份鉴别阶段不分配 IP 地址。IP 地址池耗尽是导致从网络层协议配置阶段进入 PPP 链路终止阶段的原因。

(17) 以下哪一种情况不是导致从网络层协议配置阶段进入 PPP 链路终止阶段的原因？(　　)

A. 一端发起物理链路释放过程　　B. 物理链路上检测不到载波信号

C. 用户不是注册用户　　D. IP 地址池耗尽

答案：C

【分析】 用户不是注册用户，且已经进入网络层协议配置阶段，说明建立 PPP 链路时的协商结果是无须进行身份鉴别过程，因此，用户不是注册用户不会在网络层协议配置阶段成为进入 PPP 链路终止阶段的原因。

(18) 关于 EAP，以下哪一项描述是错误的？(　　)

A. EAP 报文可以封装多种鉴别协议 PDU

B. 多种传输网络对应的链路层帧可以封装 EAP 报文

C. 鉴别协议 PDU 封装成 EAP 报文、EAP 报文封装成传输网络对应的链路层帧

D. 不存在 EAP over LAN 和 EAP over PPP

答案：D

【分析】 当 EAP 报文封装成 LAN 对应的链路层帧时，称为 EAP over LAN。当 EAP 报文封装成点对点信道对应的 PPP 帧时，称为 EAP over PPP。

(19) 以下哪一种不是 EAP 定义的报文类型？(　　)

A. 请求报文　　B. 响应报文　　C. 成功报文　　D. 鉴别报文

答案：D

【分析】 EAP 共定义了 4 种类型的报文，它们分别是请求、响应、成功和失败报文，对应的编码分别是 1～4。

(20) 关于 EAP over PPP，以下哪一项描述是错误的？(　　)

A. 互连示证者和鉴别者是点对点信道

B. PPP 帧是适合点对点信道传输的链路层帧

C. 支持多种鉴别机制

D. 鉴别协议消息直接封装成 PPP 帧

答案：D

【分析】 鉴别协议消息封装成 EAP 报文，EAP 报文封装成 PPP 帧。

(21) 关于 EAPOL 和 802.1X，以下哪一项描述是错误的？(　　)

A. 802.1X 是一种实现 LAN 环境下身份鉴别和密钥管理的协议

B. EAPOL 实现 LAN 环境下 EAP 报文传输过程

C. 鉴别协议消息封装成 EAP 报文，EAP 报文封装成 LAN 对应的链路层帧

D. 802.1X 和 EAPOL 是同义词

答案：D

【分析】 802.1X 是一种实现 LAN 环境下身份鉴别和密钥管理的协议，EAPOL 只是定义 EAP 和 LAN 之间的绑定关系。802.1X 实现身份鉴别时，将鉴别协议消息封装成 EAP 报文。然后通过 EAPOL 实现 EAP 报文示证者和鉴别者之间的传输过程。

(22) 以下哪一项不是 RADIUS 具有的功能？(　　)

A. 实现对 NAS 源端鉴别

B. 加密用户身份标识信息

C. 经过 IP 网络实现鉴别协议对应的 PDU 的传输过程

D. 建立 NAS 与鉴别服务器之间的数据传输通路

答案：D

【分析】 RADIUS 是应用层协议，建立 NAS 与鉴别服务器之间的数据传输通路不是应用层协议的功能。

(23) 以下哪一项不是鉴别服务器对应每一个 NAS 需要配置的信息？(　　)

A. 客户端名字　　　　B. 客户端 IP 地址

C. 共享密钥　　　　D. 对称密钥加密算法

答案：D

【分析】 在 RADIUS 加密用户身份标识信息过程中，只使用共享密钥和报文摘要算法。

(24) 关于 RADIUS 和统一鉴别，以下哪一项描述是错误的？(　　)

A. 鉴别者中不存储用户身份标识信息

B. 由鉴别服务器统一存储用户身份标识信息

C. 互连示证者和鉴别者是传输网络，互连鉴别者和鉴别服务器是互连网

D. RADIUS 消息直接封装成传输网络对应的链路层帧

答案：D

【分析】 由于鉴别者和鉴别服务器之间可以是互连网，互连网端到端传输的是 IP 分组，因此，RADIUS 消息需要封装成 IP 分组后，再封装成传输网络对应的链路层帧。

(25) 关于访问控制，以下哪一项描述是错误的？(　　)

A. 通过身份鉴别确定用户身份

B. 为每一个用户授权

C. 保证每一个用户只能访问授权访问的资源

D. 身份鉴别和授权控制只能由资源所在的主机完成

答案：D

【分析】 可以由独立的鉴别服务器完成身份鉴别，独立的授权服务器完成每一个用户授权，资源所在主机和鉴别服务器、授权服务器可以是不同的设备。

(26) 分布式网络环境下的 Kerberos 协议属于以下哪一项协议类型？(　　)

A. 认证协议　　　　B. 加密协议

C. 完整性检验协议　　　　D. 访问控制协议

答案：D

【分析】 Kerberos 协议用于实现分布式网络环境下的访问控制过程。

(27) 以下哪一项不是对 Kerberos 票据的正确描述？(　　)

A. 票据用于证明客户对某台服务器的访问权限

B. 客户无法解密票据

C. 票据中授权客户访问的服务器能够解密票据

D. 票据用于证明发送票据的客户的身份

答案：D

【分析】 票据不具有源端鉴别功能。客户端通过发送鉴别信息证实自己的身份。

(28) 关于 Kerberos 中鉴别服务器发送的票据，以下哪一项描述是错误的？(　　)

A. 票据由鉴别服务器与票据授权服务器之间的共享密钥加密

B. 通过票据证明某个用户的身份已经得到证实

C. 票据中含用户名和用户终端的 IP 地址

D. 票据只能使用一次

答案：D

【分析】 票据在有效期内一直有效，即在有效期内，用户只需完成一次身份鉴别过程。

(29) 关于 Kerberos 中票据授权服务器发送的票据，以下哪一项描述是错误的？(　　)

A. 票据由票据授权服务器与应用服务器之间的共享密钥加密

B. 通过票据证明某个用户的权限

C. 票据中含用户名和用户终端的 IP 地址

D. 票据只能使用一次

答案：D

【分析】 票据在有效期内一直有效，即针对同一台应用服务器，在有效期内只需完成一次权限鉴别过程。

(30) 关于 Kerberos 中的应用服务器，以下哪一项描述是错误的？(　　)

A. 存储用户需要访问的资源

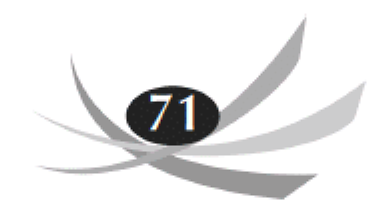
B. 用于票据授权服务器之间的共享密钥证实用户访问权限

C. 可以实现与用户之间的安全传输

D. 定义每一个用户的权限

答案：D

【分析】 每一个用户的权限是在票据授权服务器中定义的。



5.3　名 词 解 释

(1) 接入控制

只允许授权接入网络的用户所使用的终端接入网络的控制过程。

(2) 访问控制

只允许每一个用户访问授权该用户访问的网络资源的控制过程。

(3) 接入控制设备

一种既具有互连接入网络和 Internet 的功能,又具有用户终端接入控制功能的设备。

(4) 身份鉴别

验证主体的真实身份与其所声称的身份是否符合的过程。

(5) PPP

既是基于点对点信道的链路层协议,又是接入控制协议。

(6) EAP

一种和应用环境无关的、用于传输鉴别协议消息的载体协议,所有应用环境和鉴别协议都和这种载体协议绑定。

(7) RADIUS

一种可以实现接入控制设备等鉴别者与鉴别服务器之间双向身份鉴别,以及用户身份标识信息鉴别者与鉴别服务器之间安全传输的应用层协议。

(8) Kerberos

网络环境下的访问控制协议,通过单独设置身份鉴别服务器和权限鉴别服务器,使用户在某次事务中只需完成一次身份鉴别过程,对每一台应用服务器只需完成一次授权鉴别过程。

第6章 安全协议

6.1 例题解析

6.1.1 简答题解析

【例题 6.1】 简述 IPSec 和 TLS 各自适用的场景。

【解析】 IPSec 实现两个终端之间的双向身份鉴别和安全传输。安全传输的数据类型可以是直接作为 IP 分组净荷的 UDP、TCP、ICMP 报文等。

TLS 实现两个进程之间的双向身份鉴别和安全传输。安全传输的数据类型可以是直接作为 TCP 报文净荷的应用层消息,如 HTTP 消息、FTP 消息等。

如果安全要求是实现两个终端之间的双向身份鉴别和 IP 分组净荷的安全传输过程,则采用 IPSec。如果安全要求是实现两个进程之间的双向身份鉴别和 TCP 报文净荷的安全传输过程,则采用 TLS。

【例题 6.2】 对照 TLS 工作流程,回答以下问题。

(1) 如何避免访问钓鱼网站。

(2) 如何保证经过安全连接传输的数据的保密性和完整性。

(3) 如何实现源端鉴别。

【解析】

(1) 服务器完成证书申请过程,证书中给出服务器完全合格的域名与公钥之间的绑定关系。浏览器下载并安装服务器证书。浏览器鉴别服务器身份的过程就是证实服务器拥有与证书中的公钥对应的私钥的过程。

(2) 浏览器和服务器通过握手协议约定双方使用的加密算法和鉴别算法,完成加密密钥、鉴别密钥的生成过程。传输数据时,发送端通过鉴别算法和鉴别密钥生成消息鉴别码(MAC),通过加密算法和加密密钥完成对数据的加密过程。接收端通过对应的解密算法和解密密钥完成对密文的解密过程。通过鉴别算法和鉴别密钥计算出 MAC,如果接收端计算出的 MAC 与发送端发送给接收端的 MAC 相同,则表明数据传输过程中没有被篡改。

(3) 由于只有浏览器和服务器知道鉴别密钥,当一方接收到另一方发送的数据,且证明另一方根据鉴别算法和鉴别密钥计算出的 MAC 是正确的时,另一方的身份得到证实。

6.1.2 设计题解析

【例题 6.3】 如果图 6.1 中源端发送给目的端的数据经过公共网络传输时需要

保证保密性和完整性，给出安全关联参数，并给出数据经过公共网络传输时的封装格式。

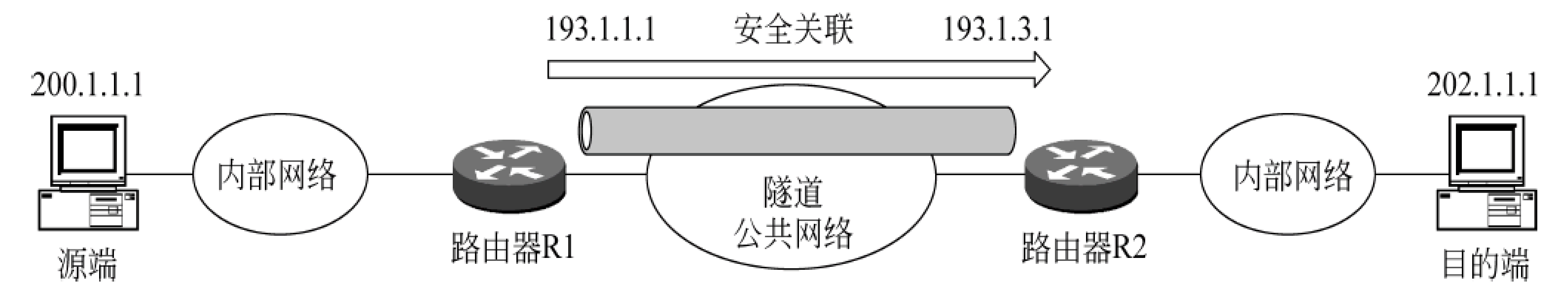


图 6.1　IP Sec 应用场景

【解析】 路由器 R1 和路由器 R2 配置信息如下。

(1) 与建立 IKE 安全关联相关的配置信息

身份鉴别机制：证书＋私钥。

加密算法：3DES。

报文摘要算法：MD5。

密钥分发协议：Diffie-Hellman，选择组号为 2 的参数。

(2) 与建立 IP Sec 安全关联相关的配置信息

安全协议：ESP。

加密算法：AES。

MAC 算法：HMAC-MD5-96。

(3) IP 分组分类标准

路由器 R1 的 IP 分组分类标准

源 IP 地址：193.1.1.1。

目的 IP 地址：193.1.3.1。

协议：GRE。

(4) 路由器 R2 的 IP 分组分类标准

源 IP 地址：193.1.3.1。

目的 IP 地址：193.1.1.1。

协议类型：GRE。

封装过程如图 6.2 所示。

【例题 6.4】 域名服务器设置如图 6.3 所示，假定终端 A 将域名服务器 dns.a.com 作为本地域名服务器，a.com 域对应的公钥和私钥分别是 PKAC 和 SKAC。b.com 域对应的公钥和私钥分别是 PKBC 和 SKBC。com 域对应的公钥和私钥分别是 PKC 和 SKC。给出实现安全的域名解析过程所需的配置和终端 A 安全地解析域名 www.b.com 的过程。

【解析】 各个域名服务器配置的资源记录如表 6.1～6.3 所示，终端 A 配置 a.com 域对应的公钥 PKAC，且公钥 PKAC 与 a.com 域之间的绑定关系已经得到验证。

安全的域名解析过程如图 6.4 所示，本地域名服务器接收到终端 A 发送的完全合格的域名 www.b.com 的解析请求后，首先在数据库中检索名字为 www.b.com、类型为 A 的资源记录。如果不存在这样的资源记录，则检索名字为 b.com、类型为 NS 的资源记

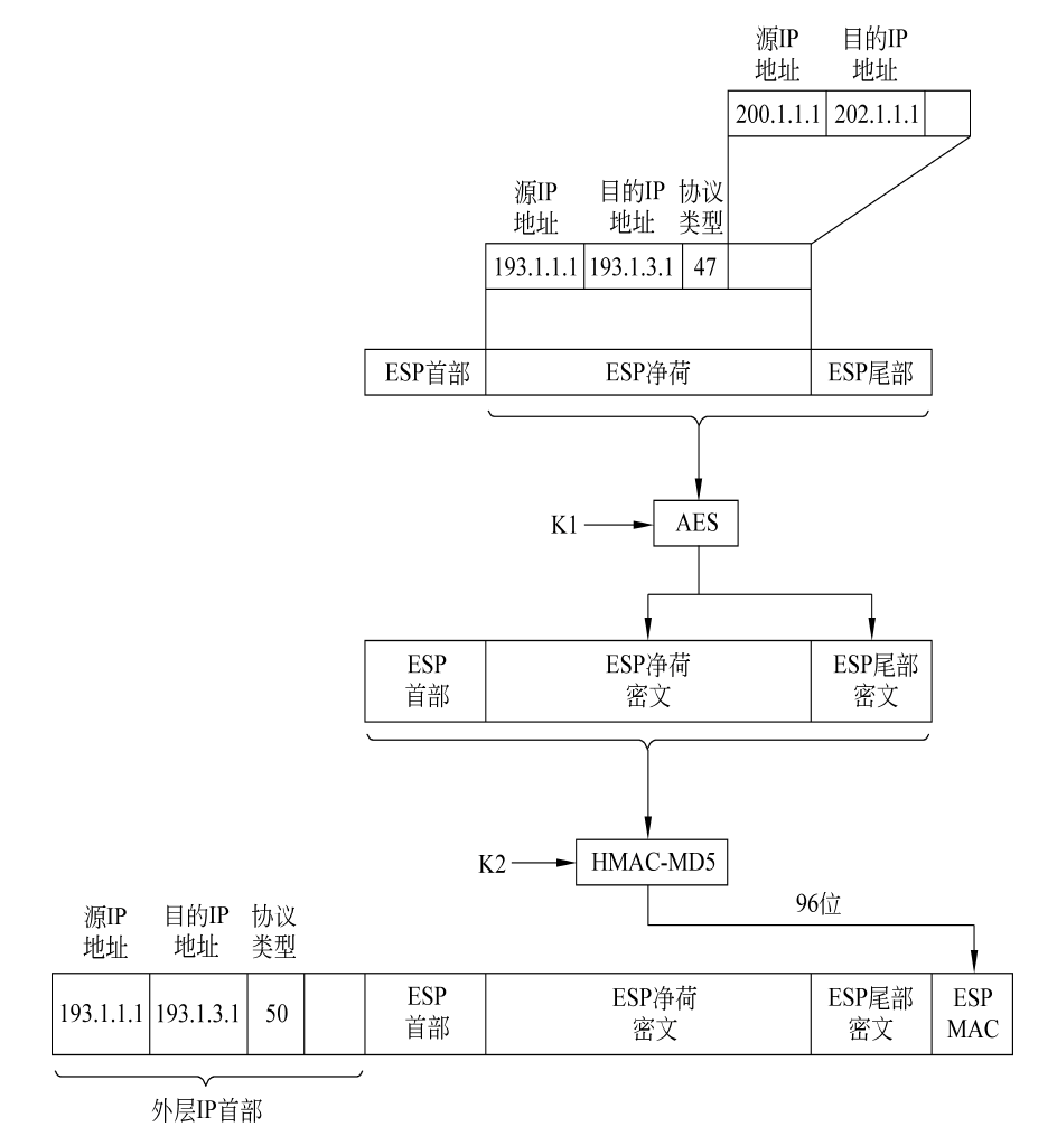


图 6.2 封装过程

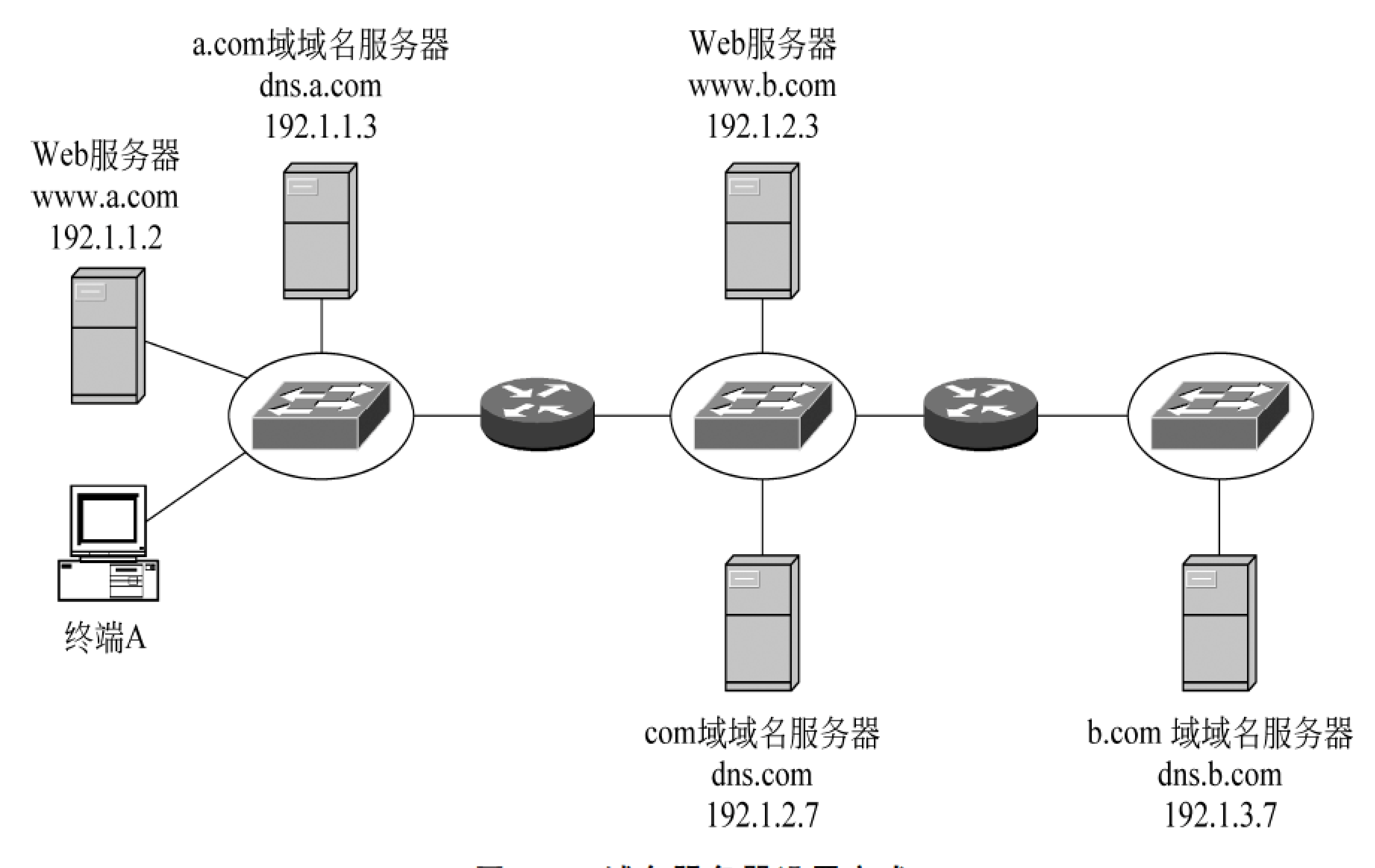


图 6.3 域名服务器设置方式

录。如果不存在这样的资源记录，则检索名字为 com、类型为 NS 的资源记录。根据资源记录＜b. com，NS，dns. com＞和＜ dns. com，A，192. 1. 2. 7＞确定 com 域域名服务器，向 com 域域名服务器发送完全合格的域名 www. b. com 的解析请求。

表 6.1　a. com 域域名服务器配置的资源记录

名　字	类　型	值
b. com	NS	dns. com
www. a. com	A	192. 1. 1. 2
dns. com	A	192. 1. 2. 7
com	DNSKEY	PKC

表 6.2　com 域域名服务器配置的资源记录

名　字	类　型	值
a. com	NS	dns. a. com
b. com	NS	dns. b. com
dns. a. com	A	192. 1. 1. 3
dns. b. com	A	192. 1. 3. 7
a. com	DNSKEY	PKAC
b. com	DNSKEY	PKBC

表 6.3　b. com 域域名服务器配置的资源记录

名　字	类　型	值
a. com	NS	dns. com
www. b. com	A	192. 1. 2. 3
dns. com	A	192. 1. 2. 7
com	DNSKEY	PKC

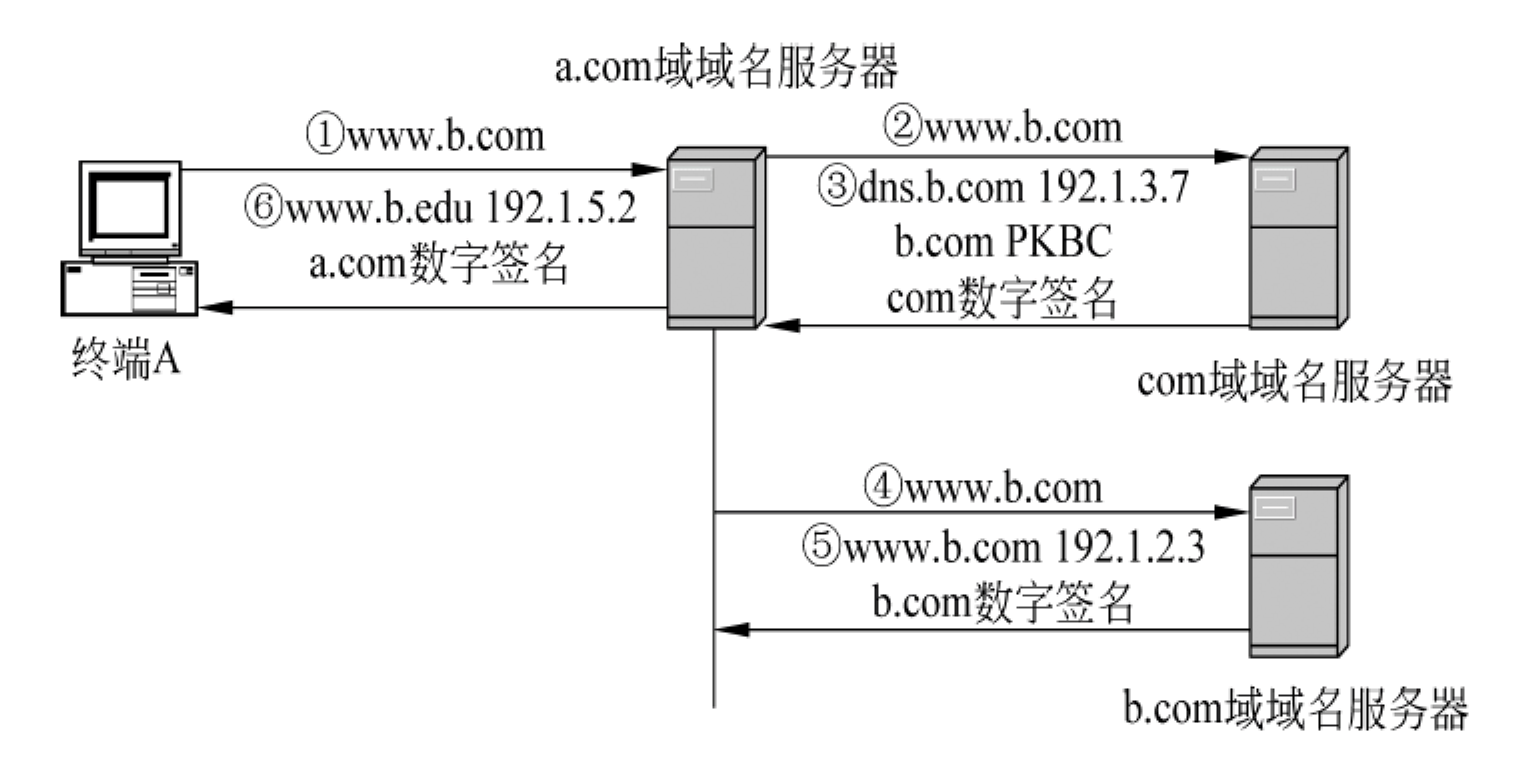


图 6.4　安全的域名解析过程

com 域域名服务器依次检索名字为 www. b. com、类型为 A 的资源记录；名字为 b. com、类型为 NS 的资源记录。根据资源记录＜b. com，NS，dns. b. com＞和＜dns. b. com，A，192. 1. 3. 7＞确定 b. com 域域名服务器，向本地域名服务器回送 b. com 域域名服务器的 IP 地址 192. 1. 3. 7、b. com 域的公钥 PKBC 和用 com 域的私钥 SKC 产生的数字签名 D_{SKC}(SHA-1((dns. b. com 192. 1. 3. 7) ‖ (b. com PKBC)))。

本地域名服务器接收到 com 域域名服务器的 DNS 响应消息后，首先用 com 域的公钥 PKC 验证 com 域域名服务器的数字签名，记录 b. com 域的公钥 PKBC。然后向 b. com 域域名服务器发送完全合格的域名 www. b. com 的解析请求。b. com 域域名服务器向本地域名服务器回送完全合格的域名为 www. b. com 的 Web 服务器的 IP 地址 192. 1. 2. 3 和用 b. com 域的私钥 SKBC 产生的数字签名 D_{SKBC}(SHA-1(www. b. com 192. 1. 2. 3))。本地域名服务器用 com 域域名服务器发送的 b. com 域的公钥 PKBC 验证 b. com 域域名服务器的数字签名。

本地域名服务器完成对 b. com 域域名服务器发送的解析结果的源端鉴别和完整性检测后，向终端 A 发送解析结果。本地域名服务器向终端 A 发送解析结果时，用 a. com 域的私钥 SKAC 产生解析结果的数字签名 D_{SKAC}(SHA-1(www. b. com 192. 1. 2. 3))。终端 A 用 a. com 域的公钥 PKAC 验证 a. com 域域名服务器的数字签名。

【例题 6.5】 对照 SET 应用系统，设计微信支付的工作流程。

【解析】 以刷卡支付和扫描支付为例，讨论微信支付的工作流程。微信支付应用系统如图 6.5 所示，微信客户端、微信支付系统和商家后台系统通过互连网连接在一起。商家门店通过商家专用网络与商家后台系统连接在一起。微信支付系统通过支付网络与各个微信支付系统支持的银行连接在一起。

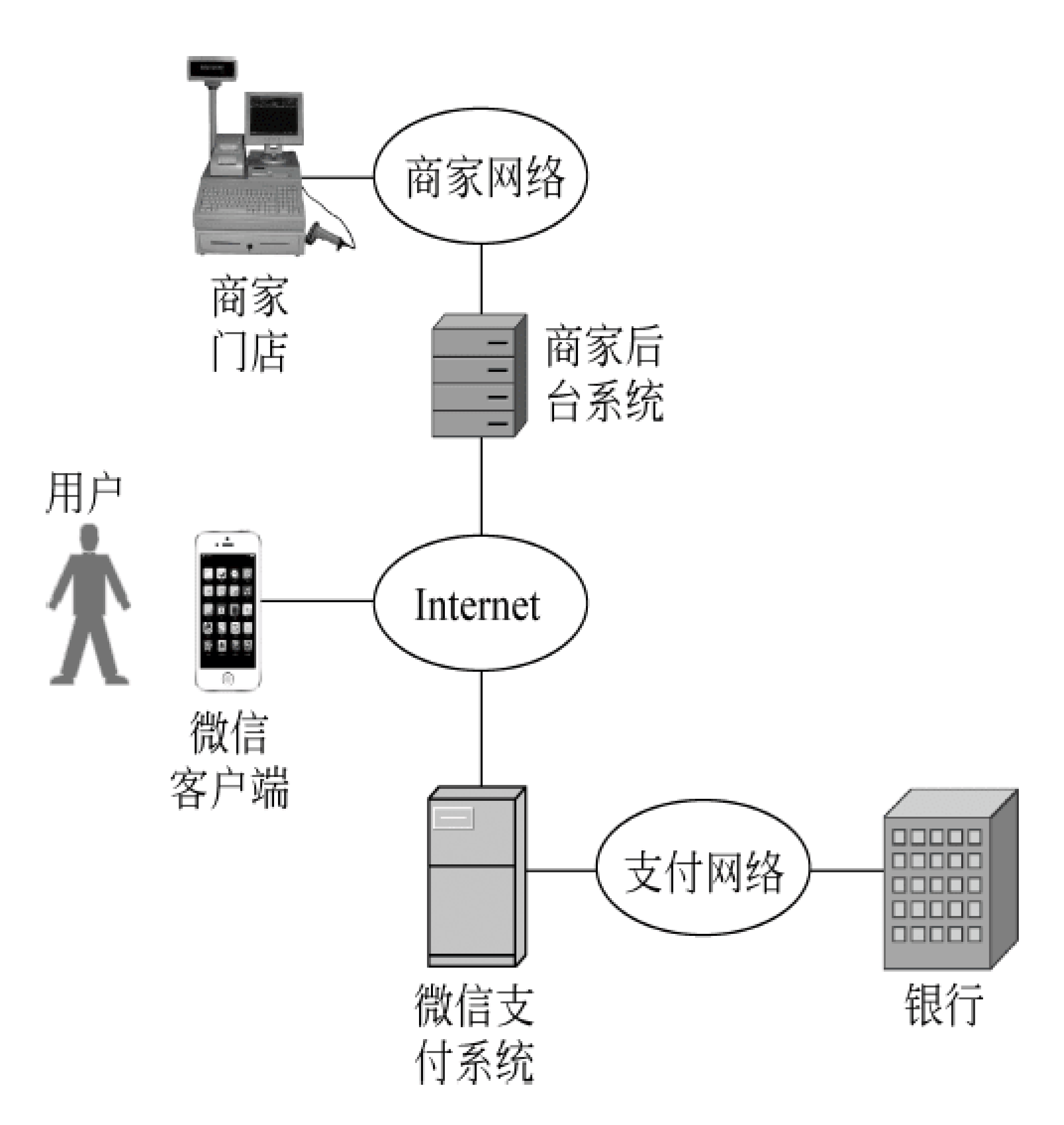


图 6.5 微信支付应用系统

微信客户端登录微信服务器端的过程如图 6.6 所示。微信客户端完成注册过程后，下载微信服务器端证书，证书中给出微信服务器端的公钥 PK。因此，微信客户端发送的登录请求是用微信服务器端的公钥 PK 加密登录信息后生成的密文 $RSAE_{PK}$(账号 ‖ 登



录密码‖K‖NONCE)。其中,RASE 是 RSA 加密算法,PK 是微信服务器端公钥,账号是微信账号,K 是微信客户端随机生成的对称密钥,NONCE 是用于验证微信服务器端身份的随机数。微信服务器端用 PK 对应的私钥 SK 还原出明文,即 $RSAD_{SK}$($RSAE_{PK}$(账号‖登录密码‖K‖NONCE))=账号‖登录密码‖K‖NONCE,其中 RSAD 是 RSA 解密算法。如果确定账号和登录密码有效,则完成登录过程,同时向微信客户端回送一个用对称密钥 K 加密随机数 NONCE 后生成的密文 $AESE_K$(NONCE),其中 AESE 是 AES 加密算法。如果微信客户端用 AES 解密算法 AESD 和对称密钥 K 解密密文后得到的明文是 NONCE,则表明微信服务器端成功获得对称密钥 K 和随机数 NONCE,以此证明微信服务器端拥有 PK 对应的私钥 SK,微信服务器端的身份得到证实。

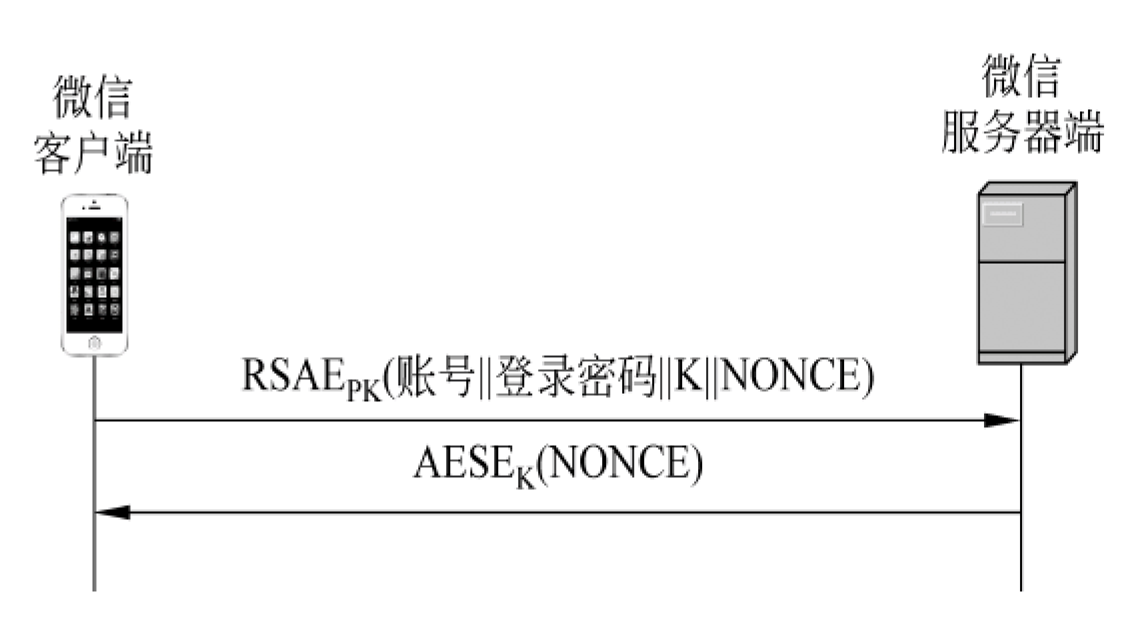


图 6.6　微信登录过程

微信刷卡支付工作流程如图 6.7 所示,当用户在商家门店完成商品选购过程后,商家门店生成订货信息,其中包括订单号、商品目录、单价和商品总价等。如果用户选择微信刷卡支付,则需要完成微信"我"→"钱包"→"刷卡"操作过程。完成上述操作过程后,微信客户端向微信支付系统发送微信授权码生成请求,微信支付系统接收到该微信授权码生成请求后,生成一个微信授权码,建立微信授权码与微信账号之间的绑定,然后将微信授权码发送给微信客户端,微信客户端上显示微信授权码的条码和二维码。商家门店扫描微信客户端上的条码或二维码,生成并向商家后台系统发送支付请求,支付请求将商家账号、订货信息与微信授权码绑定在一起。商家后台系统对支付请求进行数字签名,然后将

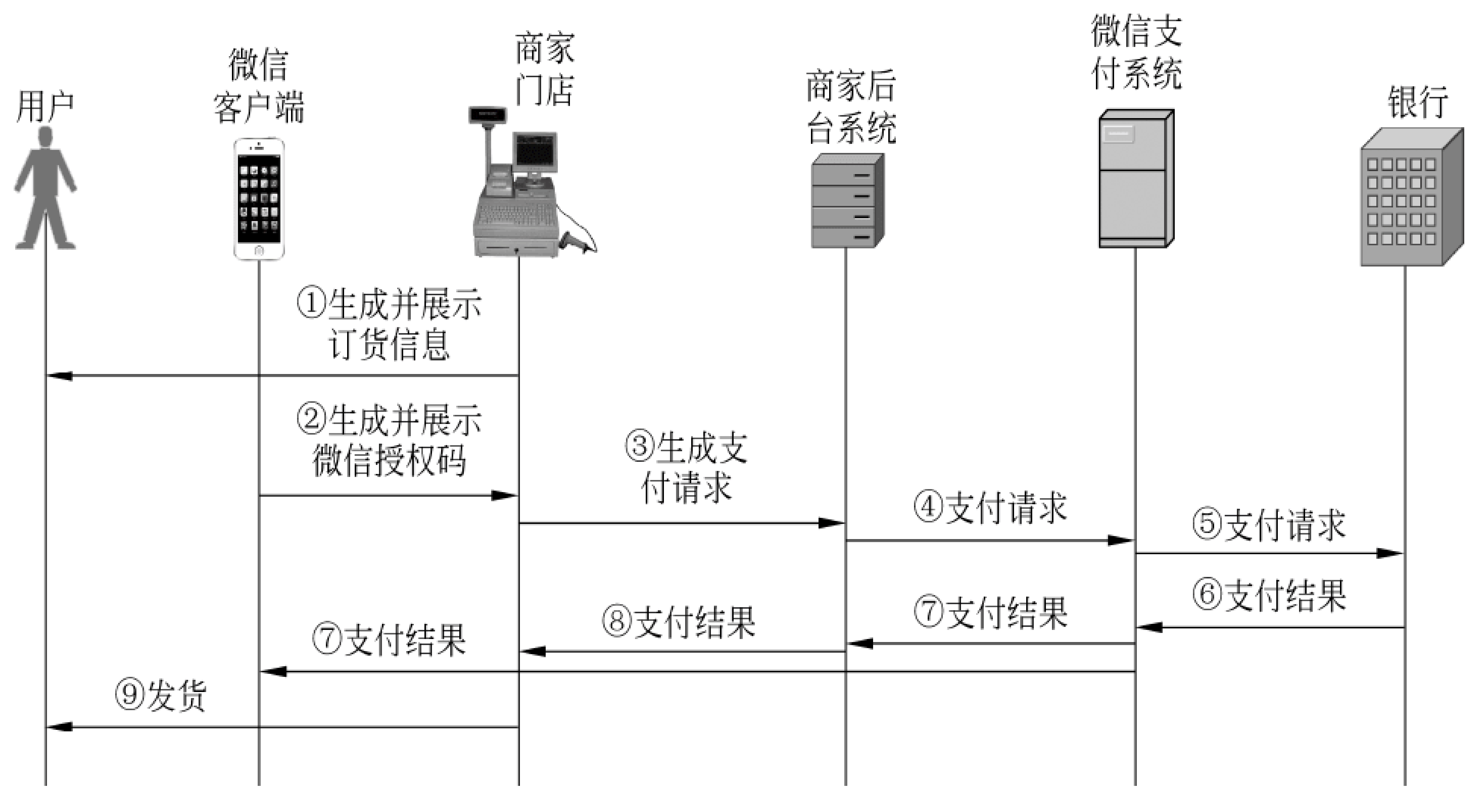


图 6.7　微信刷卡支付工作流程

数字签名后的支付请求发送给微信支付系统。微信支付系统完成支付请求源端鉴别和完整性检测后,根据微信授权码确定用户账号,根据用户账号和商家账号绑定的银行卡,请求银行完成支付过程。银行完成支付过程后,向微信支付系统发送支付结果,微信支付系统对支付结果进行数字签名,然后将数字签名后的支付结果发送给商家后台系统,支付结果中包括金额、用户账号、商家账号和订单号等信息。商家后台系统完成支付结果源端鉴别和完整性检测后,向商家门店发送支付成功的信息。微信支付系统同时也向微信客户端发送支付结果。商家门店接收到支付成功的信息后,向用户提交商品。

需要对以下几点进行说明:一是微信客户端与微信服务器端之间传输的信息都用对称密钥 K 和 AES 加密算法 AESE 进行加密;二是由商家后台系统对发送的支付请求完成以下操作。首先用商家的私钥 HSK 生成数字签名,然后随机生成对称密钥 HK,并用 AES 加密算法和对称密钥 HK 对支付请求加密,最后用微信支付系统的公钥 PK 和 RAS 加密算法对对称密钥 HK 加密,生成数字信封 $RASE_{PK}$(HK)。商家后台系统发送给支付系统的是:支付请求密文 $AESE_{HK}$(支付请求)‖数字签名 $RASD_{HSK}$(MD5(支付请求))‖数字信封 $RASE_{PK}$(HK);三是由微信支付系统对发送的支付结果完成以下操作,首先用微信支付系统的私钥 SK 生成数字签名,然后随机生成对称密钥 ZK,并用 AES 加密算法和对称密钥 ZK 对支付结果加密,最后用商家后台系统的公钥 HPK 和 RAS 加密算法对对称密钥 ZK 加密,生成数字信封 $RASE_{PK}$(ZK)。微信支付系统发送给商家后台系统的是:支付结果密文 $AESE_{ZK}$(支付结果)‖数字签名 $RASD_{SK}$(MD5(支付结果))‖数字信封 $RASE_{HPK}$(ZK)。

微信扫描支付工作流程如图 6.8 所示,当用户在商家门店完成商品选购过程后,商家门店生成订货信息,其中包括订单号、商品目录、单价和商品总价等。商家门店将订货信息发送给商家后台系统,商家后台系统生成预支付请求,预支付请求中包含商家账号和订货信息等。商家后台系统对预支付请求进行数字签名,然后将数字签名后的预支付请求发送给微信支付系统。微信支付系统完成预支付请求源端鉴别和完整性检测后,生成预

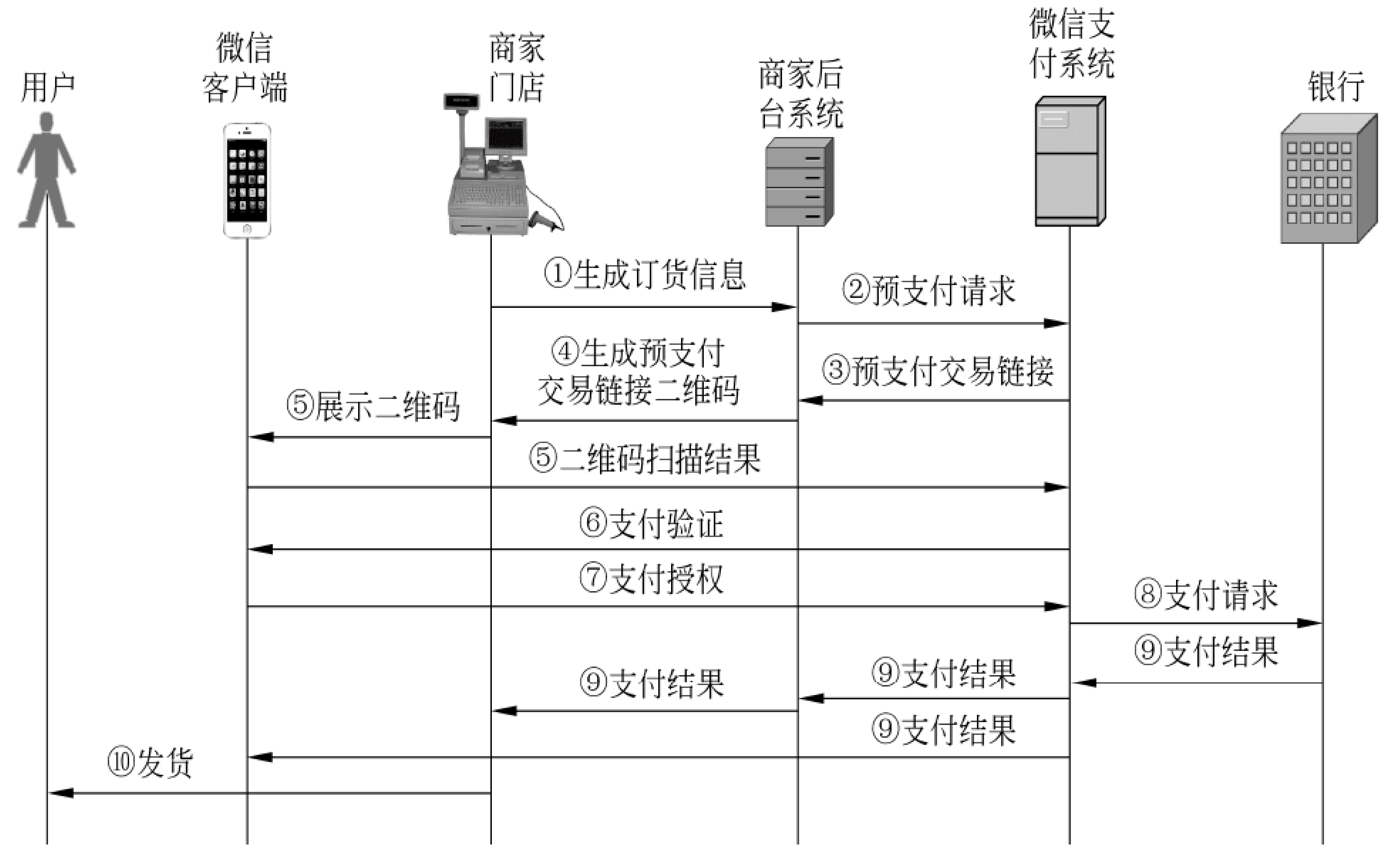


图 6.8 微信扫描支付工作流程

支付交易链接,然后将预支付交易链接发送给商家后台系统。商家后台系统生成预支付交易链接对应的二维码,将预支付交易链接对应的二维码发送给门店系统。门店系统展示预支付交易链接对应的二维码。用户用微信“扫一扫”扫描商家门店展示的预支付交易链接对应的二维码,然后将二维码扫描结果发送给微信支付系统,微信支付系统向微信客户端发送支付验证,要求用户输入支付密码。用户输入支付密码后,微信客户端向微信支付系统发送支付授权。微信支付系统确定微信客户端具有支付权限后,根据用户账号和商家账号绑定的银行卡,请求银行完成支付过程。银行完成支付过程后,向微信支付系统发送支付结果。微信支付系统对支付结果进行数字签名,然后将数字签名后的支付结果发送给商家后台系统,支付结果中包括金额、用户账号、商家账号和订单号等信息。商家后台系统完成支付结果源端鉴别和完整性检测后,向商家门店发送支付成功的信息,微信支付系统同时也向微信客户端发送支付结果。商家门店接收到支付成功的信息后,向用户提交商品。

【例题 6.6】 对照 HTTPS,设计支付宝的工作流程。

【解析】 支付宝应用系统如图 6.9 所示,与微信支付应用系统相似。对于移动支付,智能手机需要安装支付宝 App,当需要进行移动支付时,支付宝 App 需要登录支付宝网站。在支付宝 App 登录和访问支付宝网站过程中,支付宝 App 与支付宝网站之间通过 HTTPS 实现支付宝网站的身份鉴别过程和数据支付宝 App 与支付宝网站之间的安全传输过程,如图 6.10 所示。

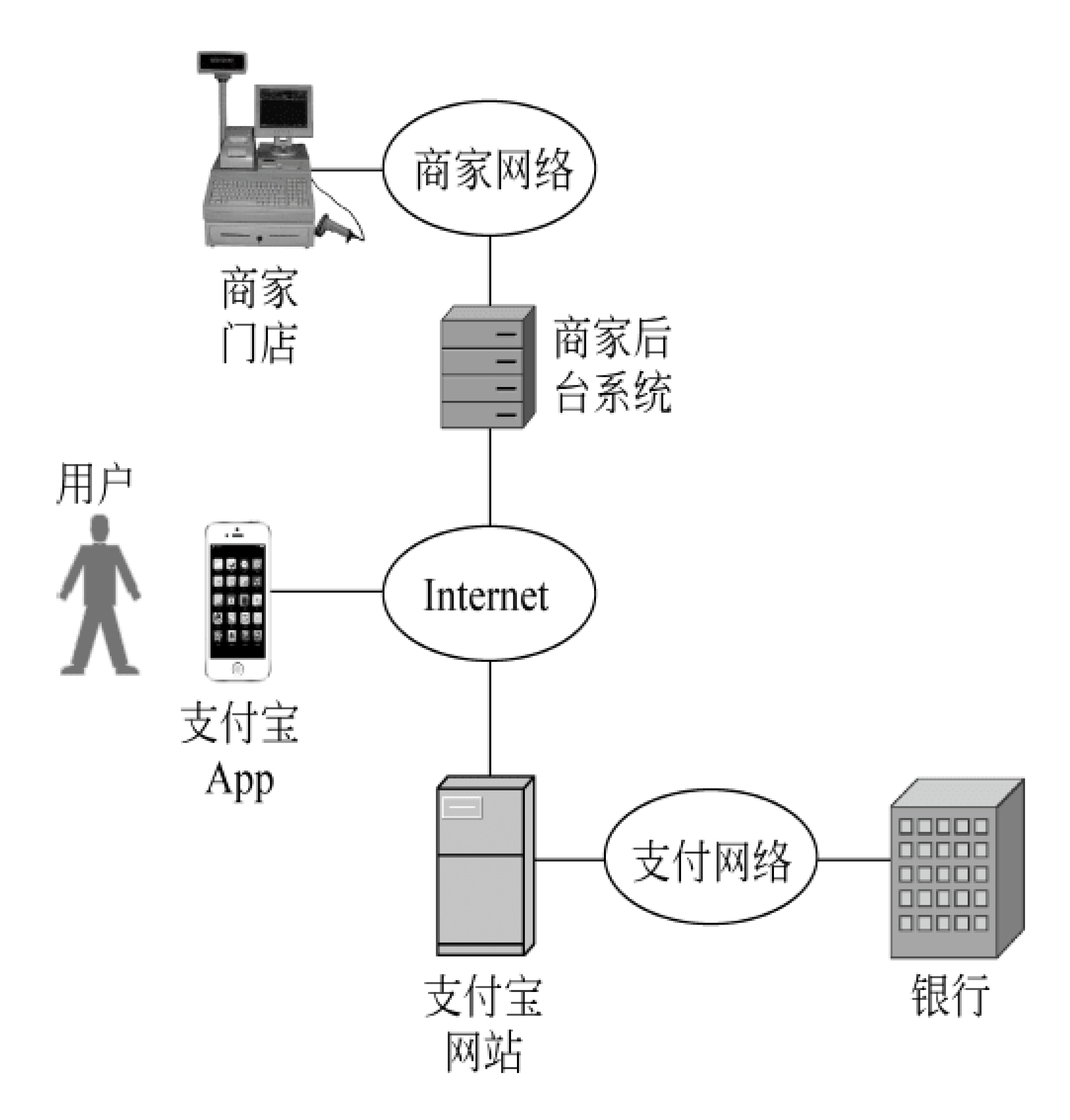


图 6.9　支付宝应用系统

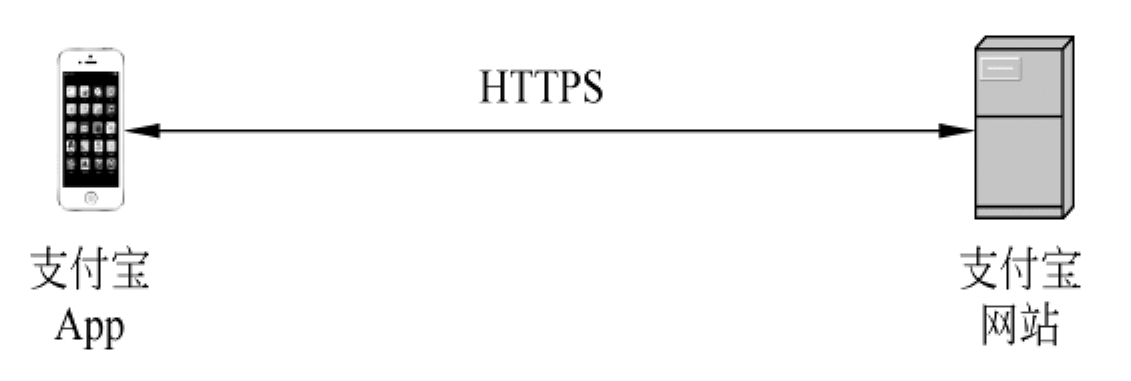


图 6.10　登录访问支付宝网站过程

6.2 选择题分析

(1) 以下哪一项不是引发安全协议的原因？(　　)

A. 冒充 IP 地址　　B. 嗅探信息

C. 篡改信息　　D. 截断信息传输路径

答案：D

【分析】 存在多种截断信息传输路径的方式，包括物理破坏方式，大部分截断信息传输路径的方式不是通过引入安全协议可以解决的。

(2) 以下哪一项不属于 IPv4 中 TCP/IP 协议栈的安全缺陷？(　　)

A. 没有为通信双方提供良好的数据源鉴别机制

B. 没有为数据提供较强的完整性保护机制

C. 没有提供复杂网络环境下的端到端可靠传输机制

D. 没有为数据提供保密性保护机制

答案：C

【分析】 TCP 已经提供了复杂网络环境下的端到端可靠传输机制。

(3) 以下哪一项不是安全协议的安全功能？(　　)

A. 双向身份鉴别　　B. 数据加密

C. 数据完整性检测　　D. 端到端可靠传输

答案：D

【分析】 端到端可靠传输涉及的内容很多，如正确的路由项、负载均衡、防御拒绝服务攻击、端到端可靠传输机制等，这些功能主要由 TCP/IP 协议栈实现。

(4) 关于重放攻击，以下哪一项描述是错误的？(　　)

A. 向接收端重复发送同一个报文　　B. 故意延长报文传输时间

C. 造成接收端报文处理出错　　D. 黑客伪造报文

答案：D

【分析】 重放攻击使用的报文的源端通常是正确的，黑客所做的是截获或嗅探报文，向接收端重复发送该报文，或者故意延迟一段时间后，再向接收端转发该报文。

(5) 以下关于 IPSec 的叙述中正确的是(　　)。

A. IPSec 是解决 IP 协议安全问题的一种方案

B. IPSec 不能提供完整性保护

C. IPSec 不能提供机密性保护

D. IPSec 不能提供认证功能

答案：A

【分析】 IPSec 实现的安全功能包括双向身份鉴别、端到端传输的数据的保密性和完整性。

(6) 以下哪一项协议不能被攻击者用来进行 DoS 攻击？(　　)

A. TCP　　B. ICMP　　C. UDP　　D. IPSec

答案：D

【分析】 IPSec是一种安全协议，其主要功能就是消除IP协议的安全缺陷。而大量的拒绝服务攻击往往是通过利用协议的安全缺陷实现的。

(7) 关于IPSec安全关联，以下哪一项描述是正确的？(　　)

A. 单向的　　B. 双向的

C. 无方向的　　D. 任意

答案：A

【分析】 IPSec安全关联是单向的，用于实现发送端至接收端的安全传输过程。如果需要实现两端之间双向安全传输过程，则必须在两端之间分别建立不同传输方向的安全关联。

(8) 以下哪一项不属于IPSec的功能？(　　)

A. 发送端鉴别　　B. 完整性检测

C. 加密传输　　D. 差错控制

答案：D

【分析】 IPSec不提供差错控制功能。

(9) 关于IPSec，以下哪一项描述是错误的？(　　)

A. IPSec是网际层实现IP分组端到端安全传输的机制

B. AH只实现数据完整性检测

C. ESP实现数据加密和完整性检测

D. 必须由IKE动态建立端到端之间的安全关联

答案：D

【分析】 端到端安全传输数据前，必须建立安全关联，但可以静态建立安全关联。

(10) 关于IPSec，以下哪一项描述是正确的？(　　)

A. AH能够实现双向身份鉴别　　B. ESP能够实现双向身份鉴别

C. IKE能够实现双向身份鉴别　　D. IP能够实现双向身份鉴别

答案：C

【分析】 在动态建立安全关联时，由IKE完成双向身份鉴别，双方可以通过共享密钥，或者证书＋私钥证实自己的身份。

(11) 关于AH，以下哪一项描述是错误的？(　　)

A. 可以检测出篡改的源IP地址

B. 可以检测出篡改的目的IP地址

C. 可以检测出篡改的IP分组净荷

D. 可以检测出篡改封装IP分组的MAC帧的源MAC地址

答案：D

【分析】 AH计算鉴别数据时，只包含IP分组中的相关字段。

(12) 以下哪一项可以验证发送终端的IP地址、保障数据的完整性和防止重放攻击？(　　)

A. AH　　B. ESP　　C. TLS　　D. SET

答案：A

【分析】 AH是唯一对源IP地址进行完整性检测的安全协议。

(13) 关于ESP,以下哪一项描述是错误的？(　　)

A. 可以检测出篡改的源IP地址

B. 可以加密IP分组净荷

C. 可以检测出篡改的IP分组净荷

D. 可以检测出篡改的ESP首部

答案：A

【分析】 ESP在计算鉴别数据时,不包含IP分组首部中传输过程中不变的字段,如源和目的IP地址。

(14) ESP协议不能对以下哪一项进行封装？(　　)

A. 应用层协议数据单元　　B. 传输层协议数据单元

C. 网络层协议数据单元　　D. 链路层协议数据单元

答案：D

【分析】 ESP是网络层安全协议,可以封装网络层及以上的PDU。

(15) 下列选项中,哪一项是ESP协议在传输模式下不进行加密的？(　　)

A. 源IP地址和目的IP地址　　B. 源端口号和目的端口号

C. 应用层协议数据　　D. ESP报尾

答案：A

【分析】 ESP协议在传输模式下不对IP分组的首部进行加密。

(16) 关于IKE,以下哪一项描述是错误的？(　　)

A. IKE第一阶段建立IKE安全关联

B. IKE第二阶段建立IPSec安全关联

C. IKE第一阶段协商加密算法和MAC算法等

D. IKE第二阶段完成双向身份鉴别过程

答案：D

【分析】 IKE在第一阶段完成双向身份鉴别过程。

(17) 以下哪一项关于TLS的描述是错误的？(　　)

A. TLS可以实现双向身份鉴别

B. TLS动态约定双方使用的安全参数

C. TLS只能用于HTTP

D. TLS握手协议是一种比较通用的双向鉴别协议

答案：C

【分析】 TLS作为传输层安全协议,可以作用于多种应用层协议。

(18) 关于TLS,以下哪一项描述是正确的？(　　)

A. 一种实现两个进程之间安全传输的安全协议

B. 一种实现两个终端之间安全传输的安全协议

C. 一种实现链路两端之间安全传输的安全协议

D. 一种与特定应用层协议相关的安全协议

答案：A

【分析】 TLS 是一种实现两个进程之间安全传输的安全协议。

(19) 关于 TLS，以下哪一项描述是错误的？(　　)

A. TLS 是一套安全协议

B. 由 TLS 握手协议完成身份鉴别和安全参数协商过程

C. 由 TLS 记录协议完成上层协议消息封装过程

D. 由 TLS 改变密码规范协议完成两端密码协商过程

答案：D

【分析】 TLS 改变密码规范协议只是用于通知对方开始使用新约定的安全参数。由 TLS 握手协议完成两端安全参数协商过程，包括两端使用的密码。

(20) 关于 HTTPS 中 TLS 的作用，以下哪一项描述是错误的？(　　)

A. 由 TLS 完成客户端对 Web 服务器的身份鉴别过程

B. 由 TLS 完成客户端与 Web 服务器之间的安全参数协商过程

C. 由 TLS 实现客户端与 Web 服务器之间的 HTTP 消息的安全传输过程

D. 由 TLS 实现客户端对 Web 服务器的访问过程

答案：D

【分析】 由 HTTP 实现客户端对 Web 服务器的访问过程，由 TLS 实现客户端与 Web 服务器之间的 HTTP 消息的安全传输过程。

(21) 以下哪一项关于 HTTPS 的描述是错误的？(　　)

A. 客户通过 TLS 鉴别服务器身份

B. 客户和服务器通过 TLS 动态约定双方使用的安全参数

C. 处理后的 HTTP PDU 作为 TLS 记录协议的净荷

D. 记录协议的内容类型字段区分不同的应用层协议

答案：D

【分析】 所有的应用层协议数据单元对应着相同的内容类型字段值，因此，不能通过记录协议的内容类型字段区分不同的应用层协议。

(22) 关于 SSL，以下哪一项描述是正确的？(　　)

A. 为链路层提供了加密、身份鉴别和完整性检测的保护

B. 为网络层提供了加密、身份鉴别和完整性检测的保护

C. 为传输层提供了加密、身份鉴别和完整性检测的保护

D. 为应用层提供了加密、身份鉴别和完整性检测的保护

答案：D

【分析】 应用层 PDU 被封装成 SSL 记录协议报文时，完成加密和计算消息鉴别码的过程。

(23) 以下哪一项不是 DNS Sec 的功能？(　　)

A. 源端鉴别

B. 完整性检测

C. 加密资源记录

D. 验证域名与 IP 地址之间的绑定关系

答案：C

【分析】 DNS Sec 不对资源记录进行加密。

(24) 关于引出 DNS Sec 的原因，以下哪一项描述是错误的？(　　)

A. 黑客可以伪造 DNS 响应消息　　B. 黑客可以篡改 DNS 响应消息

C. 黑客可以截获 DNS 响应消息　　D. 黑客可以嗅探 DNS 响应消息

答案：D

【分析】 嗅探只能获取 DNS 响应消息，有可能破坏 DNS 响应消息的保密性。一般情况下，需要保证 DNS 响应消息的真实性和完整性，但无须保证 DNS 响应消息的保密性。

(25) 关于 DNS Sec，以下哪一项描述是错误的？(　　)

A. 接收端对 DNS 响应消息实现源端鉴别

B. 接收端对 DNS 响应消息实现完整性检测

C. 发送端对 DNS 响应消息进行数字签名

D. 接收端通过 PKI 获取证明公钥与发送端之间绑定关系的证书

答案：D

【分析】 在 DNS Sec 中，每一台域名服务器需要事先获取经过验证的上一级域名服务器的公钥，并通过资源记录建立该公钥和上一级域名服务器之间的绑定关系。

(26) 以下哪一项与 DNS Sec 验证域名与 IP 地址之间的绑定关系无关？(　　)

A. 增加用于证明域名与公钥之间绑定关系的资源记录

B. 增加用于证明子域与公钥之间绑定关系的资源记录

C. 数字签名

D. 域名服务器之间用共享密钥鉴别对方身份

答案：D

【分析】 DNS Sec 通过数字签名实现 DNS 响应报文的源端鉴别和完整性检测。

(27) 安全电子交易协议 SET 是由 Visa 和 MasterCard 两大信用卡组织联合开发的电子商务安全协议。以下关于 SET 的叙述中，正确的是(　　)。

A. SET 是一种基于流密码的协议

B. SET 不需要可信的第三方认证中心的参与

C. SET 要实现的主要目标包括保障付款安全、确定应用的互通性和达到全球市场的可接受性

D. SET 通过向电子商务各参与方发放验证码确认各方的身份，保证网上支付的安全性

答案：C

【分析】 SET 采用的密码体制是分组密码体制，通过证书和私钥证明自己的身份，证书由第三方认证中心颁发。

(28) 关于 SET 中的证书，以下哪一项描述是错误的？(　　)

A. 用证书证明公钥与信用卡账号之间的绑定

B. 用证书证明公钥与商家之间的绑定

C. 认证中心提供用于验证证书的证书链

D. SET 应用系统中只允许有单个认证中心

答案：D

【分析】 SET 应用系统中允许有多个认证中心，但不同认证中心之间存在信任链，因此，可以构建验证不同认证中心颁发的证书的证书链。

(29) 以下哪一项不属于电子交易的安全需求？( )

A. 交易的真实性　　B. 交易的保密性和完整性

C. 交易的可撤销性　　D. 交易的不可抵赖性

答案：C

【分析】 电子交易的安全需求不包括交易的可撤销性。

(30) 关于 SET 应用系统中交易各方之间传输的消息，以下哪一项描述是错误的？( )

A. 接收端对消息进行源端鉴别

B. 接收端对消息进行完整性检测

C. 发送端对消息进行加密

D. 发送端和接收端事先配置用于加密的对称密钥

答案：D

【分析】 发送端随机生成用于加密消息的对称密钥，然后用接收端公钥加密对称密钥后生成数字信封，将数字信封和密文一起发送给接收端。

(31) 关于双重数字签名，以下哪一项描述是错误的？( )

A. H(H(PI)‖H(OI))的目的是不能分离订货信息和支付信息

B. 验证双重签名只需提供 H(PI)和 H(OI)

C. 可以在不提供订货信息和支付信息的情况下绑定订货信息和支付信息

D. 用发送者的私钥对 H(H(PI)‖H(OI))进行两次解密运算

答案：D

【分析】 双重签名不是指用发送者的私钥对 H(H(PI)‖H(OI))进行两次解密运算，而是对订货信息和支付信息的绑定关系进行签名。

(32) 以下哪一项不是 PGP 的功能？( )

A. 源端鉴别　　B. 加密　　C. 压缩　　D. 分发公钥

答案：D

【分析】 分发公钥不是 PGP 的功能，但 PGP 正常工作的前提是，发送端和接收端拥有对方的公钥。

(33) 关于 S/MIME，以下哪一项描述是错误的？( )

A. 基于 MIME

B. 增加了鉴别邮件子报文内容

C. 增加了加密邮件子报文内容

D. 增加了证书邮件子报文内容

答案：D

【分析】 增加的内容类型中没有单独的证书邮件子报文内容，证书包含在鉴别邮件子报文内容和加密邮件子报文内容中。

(34) 下列协议中，哪一项可以为电子邮件提供数字签名和数据加密功能？(　　)

A. SMTP　　B. S/MIME　　C. SET　　D. POP3

答案：B

【分析】 S/MIME 增加了鉴别邮件子报文内容和加密邮件子报文内容。

6.3 名词解释

(1) 安全协议

为弥补原有网络协议的安全缺陷，在原有网络协议的基础上，增加的一整套用于实现双向身份鉴别、数据传输保密性和数据传输完整性的协议。

(2) 安全协议体系结构

一种在 TCP/IP 体系结构中的每一层给出用于实现该层对等层之间安全传输过程的安全协议的体系结构。

(3) IPSec

网际层实现 IP 分组端到端安全传输的机制。

(4) 安全关联

发送者与接收者之间以实现源端鉴别、数据加密和完整性检测为目的的关联。

(5) AH

一种用于实现安全关联中发送者至接收者数据传输完整性的安全协议。

(6) ESP

一种用于实现安全关联中发送者至接收者数据传输保密性和完整性的安全协议。

(7) IKE

一种用于完成安全关联两端之间的双向身份鉴别过程和安全关联相关安全参数的协商过程的协议。

(8) TLS

一套在传输层用于完成双向身份鉴别和安全参数协商的协议。

(9) HTTPS

一种在 TCP 基础上建立 TLS 安全连接，经过 TLS 安全连接实现对 Web 服务器的身份鉴别，浏览器和 Web 服务器之间传输的 HTTP 消息的保密性、完整性和源端鉴别的安全机制。

(10) DNS Sec

在 DNS 基础上增加 DNS 响应消息源端鉴别和完整性检测的 DNS 安全协议。

(11) SET

为了解决持卡人、商家和银行之间基于 Internet 进行的电子交易过程中的安全性而

设计的协议。

(12) PGP

一种实现邮件发送端身份鉴别,保证邮件传输过程中的保密性和完整性的安全协议。

(13) S/MIME

在通用 Internet 邮件扩充(Multipurpose Internet Mail Extension,MIME)的基础上增加了和安全传输邮件相关的内容类型后的邮件格式,增加的内容类型主要是为了表示用于鉴别邮件内容的数字签名和加密邮件内容产生的密文。

第7章 以太网安全技术

7.1 例题解析

【例题7.1】 给出交换机S端口1和端口2的访问控制列表配置,使以太网满足如下安全要求。

(1) 保持如图7.1所示的连接方式不变,但允许集线器H1和H2接入其他终端。

(2) H1和H2之间只允许终端A和终端B与终端C和终端D之间相互通信。

(3) 禁止其他接入集线器的终端与连接在另一台集线器上的终端相互通信。

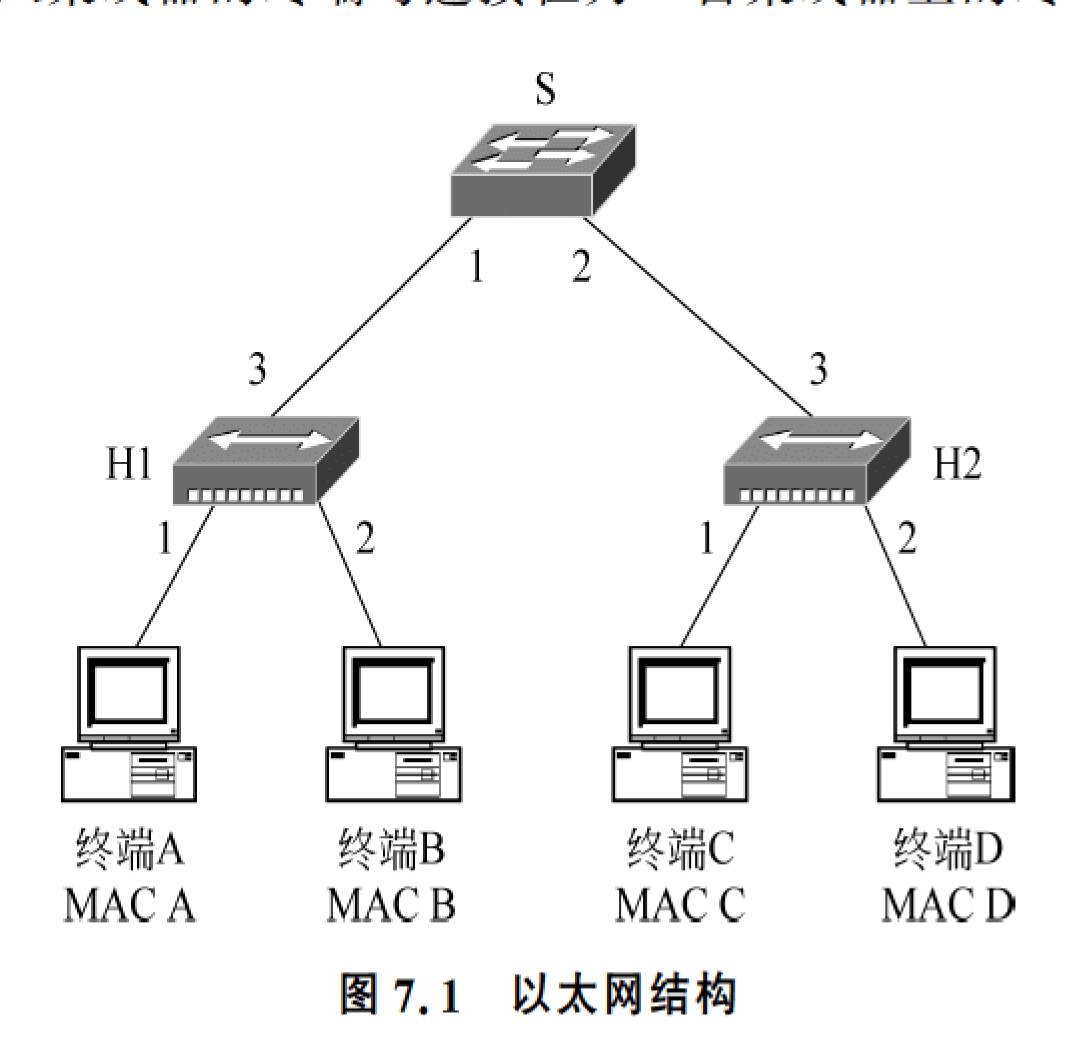


图7.1 以太网结构

【解析】 (1)启动交换机S端口1和端口2的安全功能。(2)在端口1对应的访问控制列表中配置MAC地址MAC A和MAC B,在端口2对应的访问控制列表中配置MAC地址MAC C和MAC D。(3)将端口1和端口2访问控制列表中的最大MAC地址数设置为2。

【例题7.2】 网络结构如图7.2所示,对于只需要访问内部网络资源的终端,不对其接入内部网络的过程实施控制。但只允许授权用户使用的终端访问Internet。给出用802.1X实现接入终端鉴别所需要的配置。

【解析】 在交换机S4端口1启动802.1X接入控制功能,并在交换机S4中配置如表7.1所示的鉴别数据库。

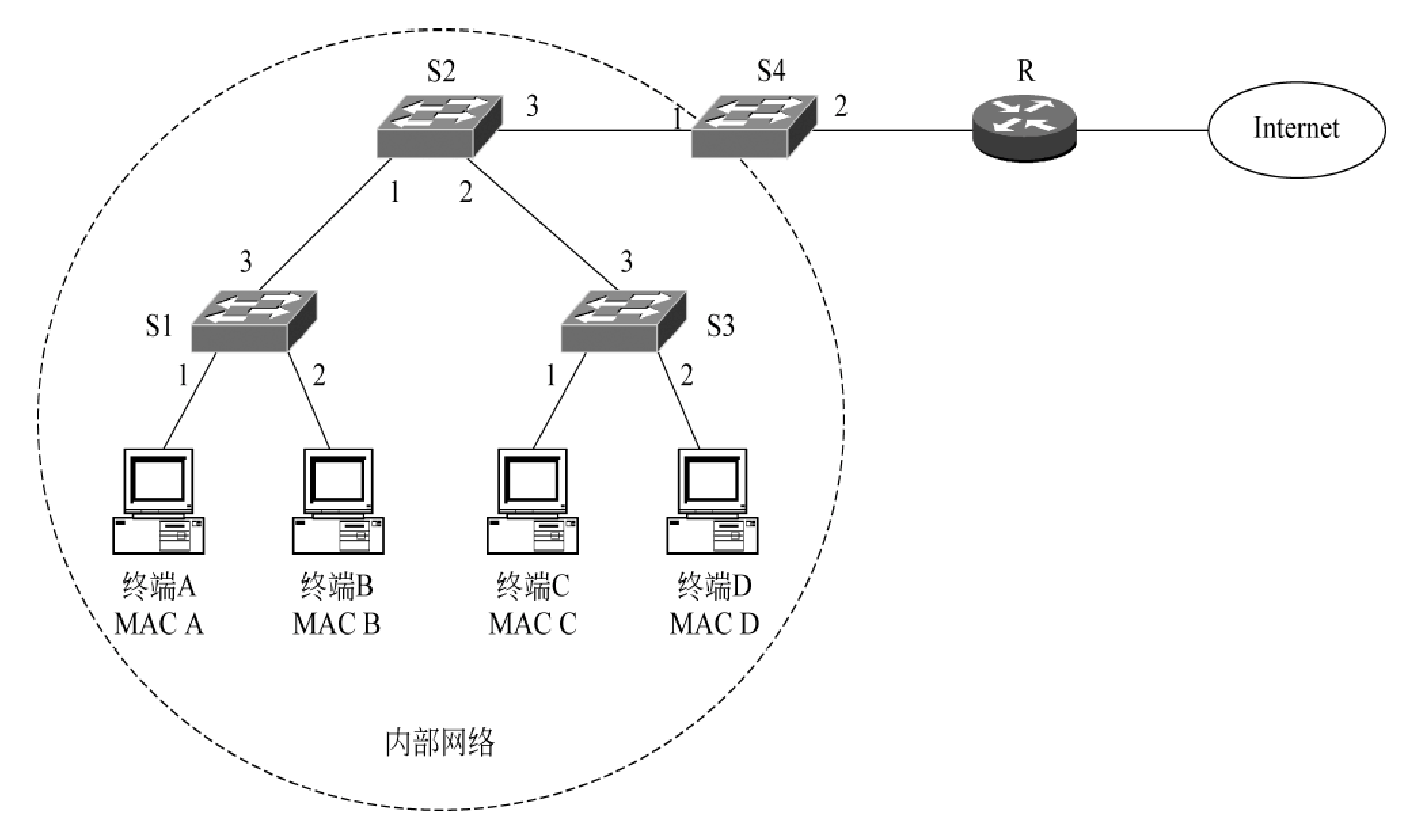


图 7.2　接入网络结构

表 7.1　鉴别数据库

用　户　名	鉴 别 机 制	口　　令
用户 A	EAP-CHAP	PASSA
用户 B	EAP-CHAP	PASSB
…		

【例题 7.3】 如果以太网结构与 DHCP 服务器配置如图 7.3 所示，确定交换机的信任端口和非信任端口。

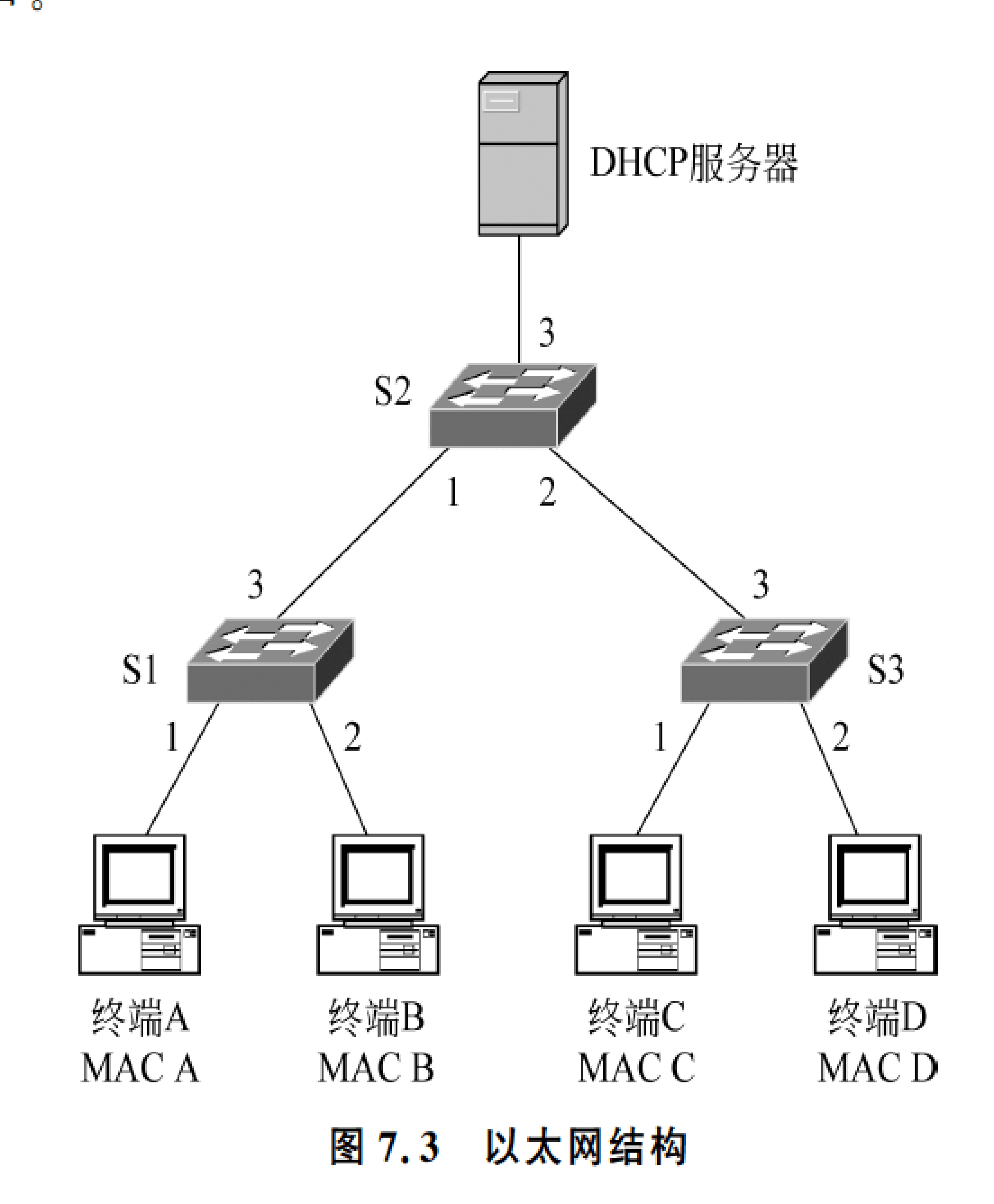


图 7.3　以太网结构

【解析】 在DHCP服务器至各个终端的交换路径所经过的交换机端口中，所有接收DHCP服务器发送的DHCP响应消息的端口都应该是信任端口，其他端口是非信任端口。因此，交换机S2端口3、交换机S1端口3和交换机S3端口3是信任端口，交换机S2端口1和端口2、交换机S1端口1和端口2及交换机S3端口1和端口2是非信任端口。

【例题7.4】 如果图7.3中的终端A、终端B、终端C和终端D通过DHCP获取的IP地址分别是IP A、IP B、IP C和IP D。给出图7.3中三台交换机的DHCP侦听信息库。

【解析】 三台交换机的DHCP侦听信息库分别如表7.2、表7.3和表7.4所示。

表7.2 交换机S1 DHCP侦听信息库

端　口	MAC地址	IP地址
1	MAC A	IP A
2	MAC B	IP B

表7.3 交换机S2 DHCP侦听信息库

端　口	MAC地址	IP地址
1	MAC A	IP A
1	MAC B	IP B
2	MAC C	IP C
2	MAC D	IP D

表7.4 交换机S3 DHCP侦听信息库

端　口	MAC地址	IP地址
1	MAC C	IP C
2	MAC D	IP D

【例题7.5】 以太网结构如图7.4所示，如果黑客终端想截获终端A和终端B与终端C和终端D之间传输的MAC帧，给出黑客终端的连接方式和配置，并简述截获过程。

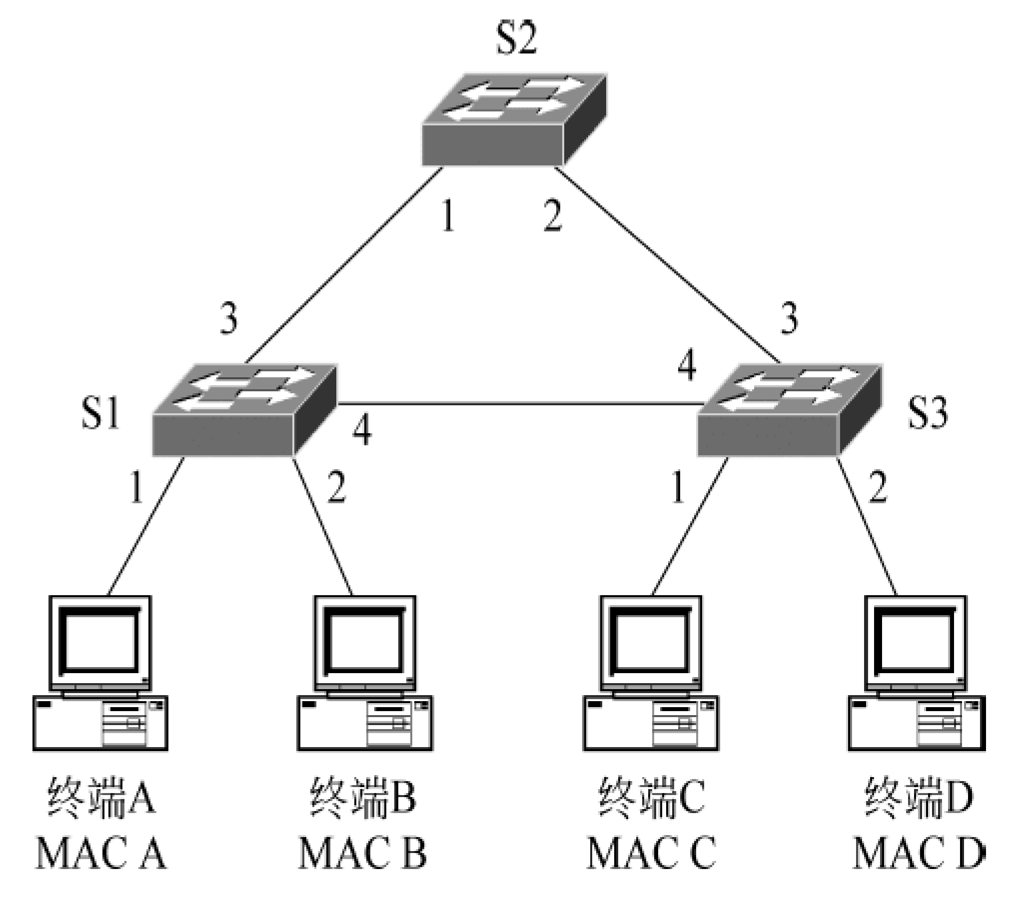


图7.4 以太网结构

【解析】 黑客终端连接方式如图 7.5(a)所示，黑客终端的两个接口分别连接交换机 S1 和 S3 的端口 5。黑客终端这样连接的目的是：当成功构建生成树，且黑客终端成为生成树的根网桥时，保证终端 A 和终端 B 与终端 C 和终端 D 之间传输的 MAC 帧经过根网桥。如图 7.5(b)所示是以黑客终端为根网桥的生成树，根据该生成树结构，终端 A 和终端 B 与终端 C 和终端 D 之间传输的 MAC 帧经过黑客终端。

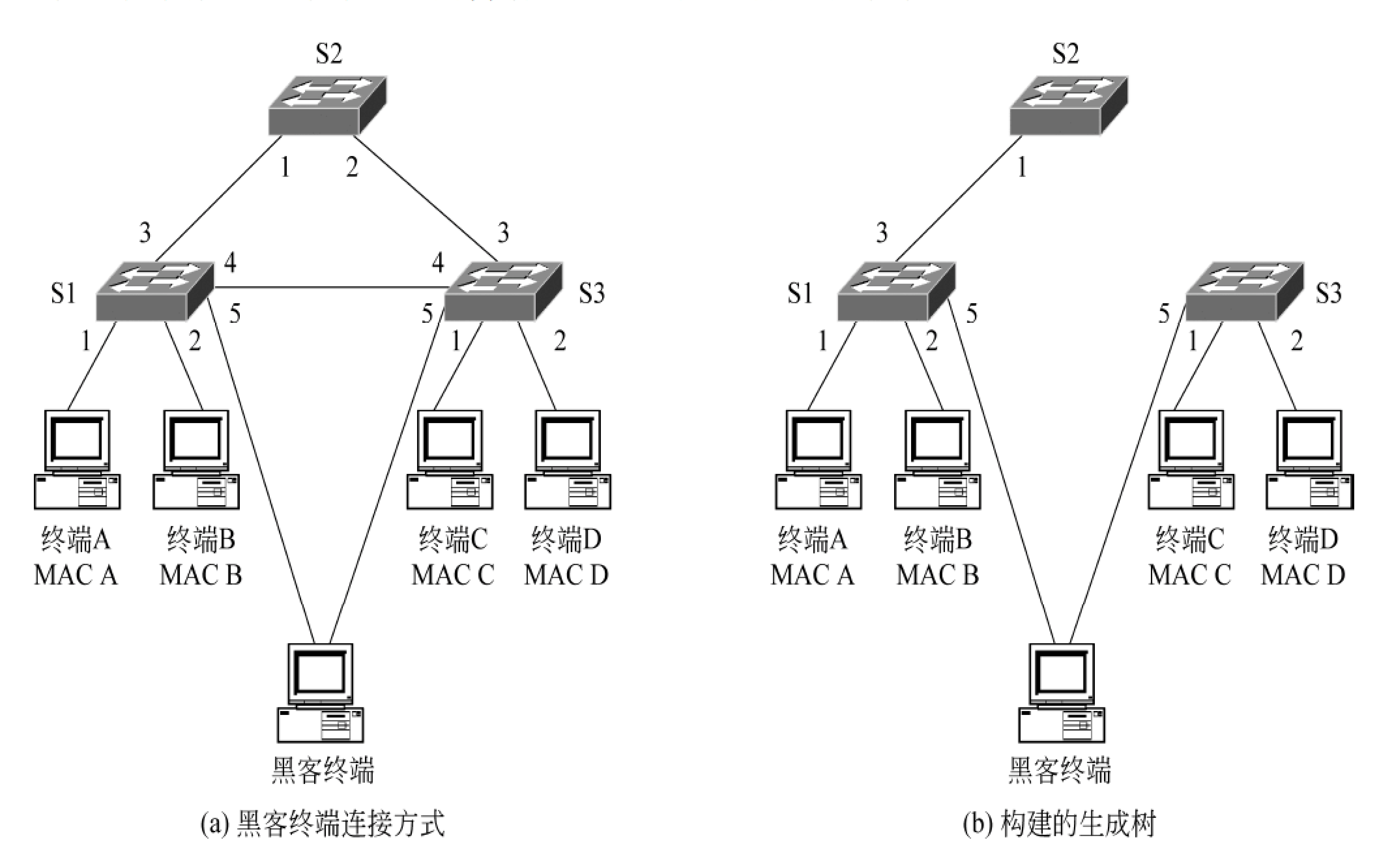


图 7.5 黑客终端连接方式和截获过程

【例题 7.6】 互连网结构如图 7.6 所示，完成以太网安全功能配置过程，使互连网具有以下安全功能。

(1) 所有终端只能从 DHCP 服务器获取网络信息。

(2) 黑客终端无法接入由交换机 S1、S2 和 S3 组成的以太网。

(3) 以太网中的终端无法实施 ARP 欺骗攻击。

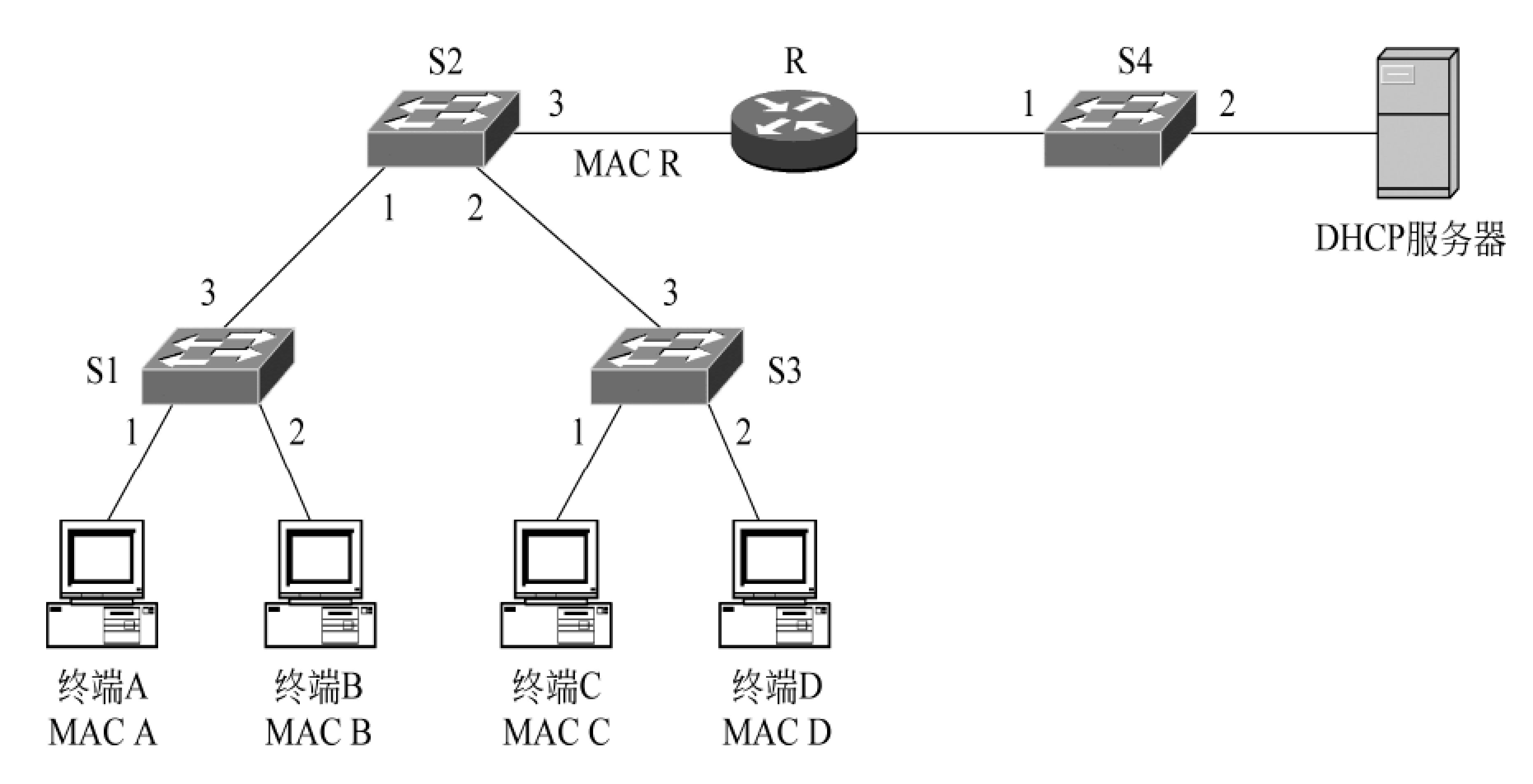


图 7.6 互连网结构

【解析】

(1) 交换机 S4 端口 2、交换机 S2 端口 3、交换机 S1 端口 3 和交换机 S3 端口 3 配置为信任端口，其他交换机端口配置为非信任端口。

(2) 除了端口 1、端口 2 和端口 3 外，关闭交换机 S1、S2 和 S3 中所有其他端口。交换机 S1 端口 1 对应访问控制列表中配置的 MAC 地址 MAC A，端口 2 对应访问控制列表中配置的 MAC 地址 MAC B，端口 3 对应访问控制列表中配置的 MAC 地址 MAC C、MAC D 和 MAC R。交换机 S2 端口 1 对应访问控制列表中配置的 MAC 地址 MAC A 和 MAC B，端口 2 对应访问控制列表中配置的 MAC 地址 MAC C 和 MAC D，端口 3 对应访问控制列表中配置的 MAC 地址 MAC R。交换机 S3 端口 1 对应访问控制列表中配置的 MAC 地址 MAC C，端口 2 对应访问控制列表中配置的 MAC 地址 MAC D，端口 3 对应访问控制列表中配置的 MAC 地址 MAC A、MAC B 和 MAC R。

(3) 启动交换机 S1、S2 和 S3 的 DHCP 侦听功能，建立 DHCP 侦听信息库。启动交换机 S1、S2 和 S3 的防 ARP 欺骗攻击功能。

7.2 选择题分析

(1) 以下哪一项不用于说明以太网安全技术的重要性？(　　)

A. 以太网是最普及的局域网之一

B. 大量安全威胁与以太网有关

C. 黑客终端常常非法接入以太网

D. 目前的以太网通常是交换式以太网

答案：D

【分析】 越普及越容易成为黑客攻击热点，因此，黑客会发明大量针对以太网的攻击方法。黑客终端实施攻击的前提是非法接入以太网。

(2) 以下哪一项攻击与以太网无关？(　　)

A. MAC 表溢出攻击　　B. MAC 地址欺骗攻击

C. 生成树欺骗攻击　　D. DNS 欺骗攻击

答案：D

【分析】 DNS 欺骗攻击与以太网无关。

(3) 以下哪一项设备不可能具备终端接入控制功能？(　　)

A. 交换机　　B. 路由器　　C. AP　　D. 总线

答案：D

【分析】 终端接入控制设备必须是智能设备。

(4) 以下哪一项设备是实施终端接入控制的最佳设备？(　　)

A. 交换机　　B. 路由器　　C. 防火墙　　D. 总线

答案：A

【分析】 接入控制最好在直接连接终端的设备上进行。

(5) 以下哪一项设备可以用于防止 DHCP 欺骗攻击?( )

A. 交换机　B. 路由器　C. AP　D. 防火墙

答案:A

【分析】 伪造的 DHCP 服务器通常需要接入以太网,且需要向以太网发送 DHCP 响应消息,因此,交换机是比较理想的禁止伪造的 DHCP 服务器向以太网发送 DHCP 响应消息的设备。

(6) 以下哪一项不是以太网的安全缺陷?( )

A. MAC 帧转发机制　B. MAC 表建立机制

C. 建立生成树机制　D. 地址解析协议

答案:D

【分析】 地址解析协议是一种通过节点的网络地址解析出节点的 MAC 地址的协议,适用于具有广播功能的网络,如以太网、无线局域网等。地址解析协议的安全缺陷会引发 ARP 欺骗攻击,但地址解析协议的安全缺陷不能作为以太网的安全缺陷。

(7) 以下哪一项是解决 MAC 表溢出攻击的有效方法?( )

A. 增加 MAC 表容量

B. 限制接入以太网的终端数量

C. 限制每一个交换机端口允许接收的源 MAC 地址不同的 MAC 帧的数量

D. 限制每一个交换机端口的数据传输速率

答案:C

【分析】 一是黑客通过发送大量源 MAC 地址不同的 MAC 帧,使交换机 MAC 表溢出;二是同一黑客终端发送的 MAC 帧,往往通过相同的交换机端口进入交换机。因此,解决 MAC 表溢出攻击的有效方法是限制每一个交换机端口允许接收的源 MAC 地址不同的 MAC 帧的数量。

(8) 以下哪一项是解决 MAC 地址欺骗攻击的有效方法?( )

A. 为每一台交换机静态配置 MAC 表

B. 对每一个 MAC 地址,永远保留第一次通过地址学习建立的转发项

C. 取消更新转发项的功能

D. 每一个交换机端口只允许接收源 MAC 地址是合法地址的 MAC 帧

答案:D

【分析】 其他三项需要改变交换机建立 MAC 表的机制,这些改变会导致终端之间无法通信。D 选项使黑客终端无法有效接入交换机端口。

(9) 以下哪一项是解决 DHCP 欺骗攻击的有效方法?( )

A. 终端具有鉴别 DHCP 服务器功能

B. 终端只向正确的 DHCP 服务器发送 DHCP 服务请求

C. 交换机端口具有鉴别 DHCP 服务器功能

D. 限制允许接入 DHCP 服务器的交换机端口

答案:D

【分析】 为了保证只允许正确的 DHCP 服务器接入以太网,让正确的 DHCP 服务

器接入指定的交换机端口,禁止其他端口连接的服务器提供 DHCP 服务,即禁止其他端口连接的服务器发送 DHCP 响应消息。

(10) 以下哪一项是防止源 IP 地址欺骗攻击的有效手段?( )

A. 绑定 MAC 地址和 IP 地址　　B. 绑定接入端口和 MAC 地址

C. 绑定接入端口和 IP 地址　　D. 防火墙设置标准过滤器

答案:C

【分析】 将 IP 地址和交换机端口绑定,从该交换机端口输入的 IP 分组中,只允许继续传输源 IP 地址为与该交换机端口绑定的 IP 地址的 IP 分组是防止源 IP 地址欺骗攻击的有效手段。

(11) 以下哪一项是可以防止 ARP 欺骗攻击的手段?( )

A. 绑定 MAC 地址和 IP 地址　　B. 绑定接入端口和 MAC 地址

C. 绑定接入端口和 IP 地址　　D. 防火墙设置标准过滤器

答案:A

【分析】 ARP 欺骗攻击就是通过伪造 IP 地址与 MAC 地址之间的绑定关系实施的。

(12) 访问控制列表是基于以下哪一项的接入控制技术?( )

A. 终端 MAC 地址　　B. 注册用户的用户名和口令

C. 终端 IP 地址　　D. MAC 帧类型

答案:A

【分析】 某个交换机端口一旦配置 MAC 地址列表,则在该交换机端口输入的 MAC 帧中,只允许继续传输源 MAC 地址属于 MAC 地址列表中的 MAC 地址的 MAC 帧。

(13) 以下哪一项有关 802.1X 的描述是错误的?( )

A. 802.1X 是基于用户的接入控制技术

B. 802.1X 和访问控制列表结合才能精细控制终端接入过程

C. 终端多次接入某个交换机端口只需一次身份鉴别过程

D. 身份鉴别过程中记录授权用户使用的终端的 MAC 地址

答案:C

【分析】 一旦交换机端口检测到该终端离线,或者在规定时间内没有接收到该终端发送的 MAC 帧,则在重新通过身份鉴别前,该交换机端口将禁止转发该终端发送的 MAC 帧。

(14) 以下哪一项是解决 ARP 欺骗攻击的有效方法?( )

A. 为每一个终端静态配置 IP 地址与 MAC 地址之间的绑定关系

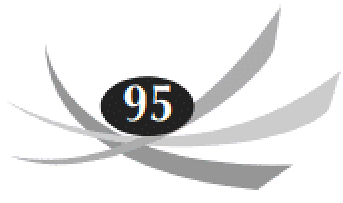
B. 每一个终端具有判别任何 IP 地址和 MAC 地址对是否有效的能力

C. 每一个终端具有 ARP 报文源端鉴别的能力

D. 交换机建立每一个端口连接的终端的 IP 地址和 MAC 地址对

答案:D

【分析】 IP 地址是逻辑地址,随着终端连接的网络不同而不同,MAC 地址是物理地址,与网卡绑定。因此,IP 地址与 MAC 地址之间的绑定关系是变化的。连接终端的交换



机端口可以检测终端 IP 地址与 MAC 地址之间的动态绑定关系，并因此发现 ARP 欺骗攻击。

(15) 以下哪一项是解决生成树欺骗攻击的有效方法？(　　)

A. 构建一个交换机之间不存在环路的以太网

B. 交换机停止运行生成树协议

C. 精心配置交换机与生成树相关的参数

D. 只允许互连有效交换机的交换机端口发送和接收 BPDU

答案：D

【分析】 实施生成树欺骗攻击的黑客终端，一是通过配置多个与属于不同交换机的端口互连的接口，使以太网成为网状型拓扑结构；二是通过极端配置，使黑客终端成为生成树根交换机。因此，解决生成树欺骗攻击的有效方法是不允许黑客终端参与构建生成树过程，即连接黑客终端的交换机端口禁止发送和接收 BPDU。

(16) 关于静态配置访问控制列表，以下哪一项描述是正确的？(　　)

A. 只允许交换机端口接收和转发目的 MAC 地址是指定 MAC 地址的 MAC 帧

B. 只允许交换机端口接收和转发源 MAC 地址是指定 MAC 地址的 MAC 帧

C. 只允许交换机端口接收和转发源和目的 MAC 地址是指定 MAC 地址的 MAC 帧

D. 只允许交换机端口接收和转发指定类型的 MAC 帧

答案：B

【分析】 只允许交换机端口接收和转发源 MAC 地址是访问控制列表中的 MAC 地址的 MAC 帧。

(17) 在以下攻击中，哪一项攻击是静态配置访问控制列表无法防御的？(　　)

A. MAC 表溢出攻击　　B. MAC 地址欺骗攻击

C. DHCP 欺骗攻击　　D. ARP 欺骗攻击

答案：D

【分析】 静态配置访问控制列表能够防御的攻击通常是通过伪造源 MAC 地址实施的攻击，如 MAC 表溢出攻击和 MAC 地址欺骗攻击，由于静态配置访问控制列表可以限制接入交换机端口的服务器的 MAC 地址，因此，也具有禁止没有允许接入的 DHCP 服务器接入的功能。ARP 欺骗攻击是伪造 IP 地址与 MAC 地址之间的绑定关系，因此，无法通过静态配置访问控制列表实现防御。

(18) 关于安全端口，以下哪一项描述是正确的？(　　)

A. 静态配置访问控制列表中的 MAC 地址

B. MAC 表中最先通过地址学习过程学习到的 n 个 MAC 地址构成访问控制列表

C. 访问控制列表中的 MAC 地址是不断变化的

D. 访问控制列表一直与 MAC 表保持同步

答案：B

【分析】 在安全端口方式下，访问控制列表中的 n 个 MAC 地址是 MAC 表中最先通过地址学习过程学习到的 n 个 MAC 地址。但一旦访问控制列表中的 MAC 地址数达到最大地址数 n，访问控制列表中的 MAC 地址不再发生变化。

(19) 关于安全端口，以下哪一项描述是正确的？(　　)

A. 安全端口比静态配置访问控制列表安全

B. 黑客终端的 MAC 地址可能成为访问控制列表中的 MAC 地址

C. 静态配置访问控制列表比安全端口方便

D. 安全端口比静态配置访问控制列表更能精确地控制终端接入

答案：B

【分析】 在安全端口方式下，访问控制列表中的 n 个 MAC 地址是 MAC 表中最先通过地址学习过程学习到的 n 个 MAC 地址。这就无法保证这 n 个 MAC 地址就是 n 个允许接入交换机的终端的 MAC 地址。安全端口的好处是自动获取访问控制列表中的 MAC 地址。

(20) 关于 802.1X 接入控制过程，以下哪一项描述是错误的？(　　)

A. 允许授权用户使用的终端接入

B. 用用户名和口令标识授权用户

C. 需要运行客户端程序

D. 允许特定 MAC 地址的终端接入

答案：D

【分析】 802.1X 允许终端接入的条件如下：一是运行客户端程序；二是需要对客户端程序输入某个授权用户对应的用户名和口令。该终端的 MAC 地址与是否允许该终端接入无关。

(21) 关于 802.1X 接入控制过程和访问控制列表，以下哪一项描述是错误的？(　　)

A. 访问控制列表中是授权用户使用的终端的 MAC 地址

B. 访问控制列表中是静态配置的特定终端的 MAC 地址

C. 完成身份鉴别过程后，发起身份鉴别过程的终端的 MAC 地址进入访问控制列表

D. 完成身份鉴别过程后，用 MAC 地址标识授权用户使用的终端

答案：B

【分析】 如果成功完成身份鉴别过程，将身份鉴别过程中封装身份标识信息的 MAC 帧的源 MAC 地址作为标识授权用户使用的终端的 MAC 地址，将该 MAC 地址放入访问控制列表，以后，交换机端口允许接收和转发以该 MAC 地址为源 MAC 地址的 MAC 帧。

(22) 关于统一鉴别和本地鉴别，以下哪一项描述是错误的？(　　)

A. 在统一鉴别方式下，交换机需要配置鉴别服务器的 IP 地址

B. 在本地鉴别方式下，交换机需要配置允许接入的授权用户的身份标识信息

C. 在统一鉴别方式下，统一在鉴别服务器中配置允许接入的授权用户的身份标识信息

D. 在本地鉴别方式下，某个授权用户只能接入单台指定交换机

答案：D

【分析】 在本地鉴别方式下，某个授权用户允许接入多台不同的交换机，只是这些交换机中都需要配置该授权用户的身份标识信息。

(23) 关于统一鉴别方式下的交换机与鉴别服务器，以下哪一项描述是错误的？(　　)

A. 鉴别过程中相互交换的鉴别信息通常封装成 RADIUS 消息

B. 交换机和鉴别服务器都需要配置交换机与鉴别服务器之间的共享密钥

C. 交换机和鉴别服务器都需要配置对方的 IP 地址

D. 交换机需要对发送的 RADIUS 消息进行数字签名

答案：D

【分析】 交换机和鉴别服务器通过它们之间的共享密钥实现源端鉴别。

(24) 如果直接连接在某个交换机端口的终端已经成功完成 802.1X 接入控制过程，则以下哪一项描述是错误的？(　　)

A. 删除交换机端口与终端之间的连接线，该端口的访问控制列表中删除该终端的 MAC 地址

B. 终端长时间不发送 MAC 帧，该端口的访问控制列表中删除该终端的 MAC 地址

C. 终端通过客户端程序完成退出过程，该端口的访问控制列表中删除该终端的 MAC 地址

D. 终端发送数据的速率超过阈值，该端口的访问控制列表中删除该终端的 MAC 地址

答案：D

【分析】 802.1X 接入控制过程本身没有带宽控制功能，只要使用终端的用户是授权用户，且终端一直在线，连接该终端的交换机端口的访问控制列表中一直存在该终端的 MAC 地址。在线是指终端与交换机端口之间的物理连接一直存在，且终端没有长时间不发送 MAC 帧。

(25) 关于以太网防御 DHCP 欺骗攻击机制，以下哪一项描述是正确的？(　　)

A. 终端对 DHCP 响应消息进行源端鉴别

B. 交换机端口对应的访问控制列表中配置允许接入的 DHCP 服务器的 MAC 地址

C. 交换机只继续转发从信任端口接收到的 DHCP 响应消息

D. 交换机对 DHCP 服务器进行身份鉴别

答案：C

【分析】 交换机端口配置成信任端口和非信任端口，交换机只继续转发从信任端口接收到的 DHCP 响应消息。

(26) 关于 DHCP 侦听，以下哪一项描述是错误的？(　　)

A. 交换机记录下 DHCP 请求消息中的 MAC 地址、接收 DHCP 请求消息的端口号及端口所属的 VLAN 等信息

B. 交换机根据从信任端口接收到的 DHCP 响应消息中的 MAC 地址匹配相应项，覆盖相应项中的 IP 地址等

C. 终端自动获取网络信息后，交换机自动记录该终端的 IP 地址和 MAC 地址对

D. 交换机根据封装 DHCP 消息的 MAC 帧的源和目的 MAC 地址确定 DHCP 请求消息和响应消息

答案：D

【分析】 将 DHCP 消息封装成 UDP 报文，交换机根据 UDP 报文的源和目的端口号确定是 DHCP 消息，通过分析 DHCP 消息的首部字段确定是请求消息或响应消息。

(27) 关于以太网防御 ARP 欺骗攻击机制，以下哪一项描述是正确的？(　　)

A. 终端对 ARP 报文进行源端鉴别

B. 交换机端口对应的访问控制列表中配置该端口直接连接的终端的 MAC 地址

C. 交换机在 DHCP 侦听信息库中匹配 ARP 报文中的 IP 地址和 MAC 地址对

D. 交换机只继续转发从信任端口接收到的 ARP 报文

答案：C

【分析】 只要交换机启动 DHCP 侦听功能，且终端通过 DHCP 自动获取网络信息，交换机 DHCP 侦听库中自动记录下该终端的 IP 地址和 MAC 地址对。如果 ARP 报文中的 IP 地址和 MAC 地址对无法匹配 DHCP 侦听库中记录的所有 IP 地址和 MAC 地址对，则表明该 ARP 报文中的 IP 地址和 MAC 地址对是伪造的。

(28) 关于以太网防御源 IP 地址欺骗攻击机制，以下哪一项描述是正确的？(　　)

A. 用 IP 分组的源 IP 地址和封装该 IP 分组的 MAC 帧的源 MAC 地址匹配 DHCP 侦听信息库中的 IP 地址和 MAC 地址对

B. 用 IP 分组的源 IP 地址和封装该 IP 分组的 MAC 帧的目的 MAC 地址匹配 DHCP 侦听信息库中的 IP 地址和 MAC 地址对

C. 用 IP 分组的目的 IP 地址和封装该 IP 分组的 MAC 帧的源 MAC 地址匹配 DHCP 侦听信息库中的 IP 地址和 MAC 地址对

D. 用 IP 分组的目的 IP 地址和封装该 IP 分组的 MAC 帧的目的 MAC 地址匹配 DHCP 侦听信息库中的 IP 地址和 MAC 地址对

答案：A

【分析】 如果源 IP 地址不是伪造的，则 DHCP 侦听信息库中存在与该 IP 分组的源 IP 地址和封装该 IP 分组的 MAC 帧的源 MAC 地址匹配的 IP 地址和 MAC 地址对。

(29) 以下哪一项有关生成树协议的描述是错误的？(　　)

A. 生成树协议允许网状以太网结构

B. 生成树协议允许在存在环路的以太网中传输 MAC 帧

C. 生成树协议通过阻塞一些交换机端口以消除环路且保证连通性

D. 生成树协议自动根据以太网拓扑结构变化调整交换机端口状态

答案：B

【分析】 生成树协议的作用是将网状以太网转变成树形以太网,然后让交换机在树形以太网结构中转发MAC帧。

(30) 关于以太网防御生成树欺骗攻击机制,以下哪一项描述是正确的?(　　)

A. 交换机对BPDU进行源端鉴别

B. 交换机对发送的BPDU进行数字签名

C. 交换机禁止连接终端的端口发送接收BPDU

D. 交换机之间相互鉴别对方身份

答案:C

【分析】 实施生成树欺骗攻击的前提如下:一是黑客终端用多个接口连接多个属于不同交换机的端口;二是黑客终端将自己配置成优先级最高的交换机;三是黑客终端与交换机之间正常交换BPDU。交换机禁止连接终端的端口发送接收BPDU,使黑客终端与交换机之间无法交换BPDU,黑客终端因而也无法成为生成树的根网桥。

(31) 关于虚拟局域网防御攻击的机制,以下哪一项描述是错误的?(　　)

A. 将一个大的广播域划分为多个相对小的独立的广播域

B. 使黑客终端和攻击目标不在同一个广播域

C. 每一个VLAN有着独立的MAC表

D. 不同VLAN之间不能相互通信

答案:D

【分析】 大量攻击行为局限在广播域内,因此,缩小广播域可以缩小这些攻击的危害范围。划分VLAN是将一个大的广播域划分为多个相对小的独立的广播域。不同VLAN之间是可以在网际层实现相互通信的。

(32) 关于虚拟局域网防御攻击的功能,以下哪一项描述是错误的?(　　)

A. 缩小ARP欺骗攻击的范围　　B. 缩小MAC表溢出攻击的范围

C. 缩小MAC地址欺骗攻击的范围　　D. 缩小DNS欺骗攻击的范围

答案:D

【分析】 DNS欺骗攻击范围是互连网,不是可以通过划分VLAN缩小的。

(33) 以下哪一项不是划分VLAN的原因?(　　)

A. 缩小广播域

B. 便于控制VLAN间交换的数据

C. 缩小ARP欺骗攻击的攻击范围

D. 缩小源IP地址欺骗攻击的攻击范围

答案:D

【分析】 划分VLAN并不能缩小源IP地址欺骗攻击的攻击范围。

7.3 名词解释

(1) 访问控制列表

交换机端口对应的MAC地址列表,启动该交换机端口的安全功能后,该交换机端口

只允许接收并转发源 MAC 地址属于对应的 MAC 地址列表的 MAC 帧。

(2) 安全端口

一种自动建立访问控制列表的机制，将 MAC 表中针对某个端口最先通过地址学习过程学习到的 n 个 MAC 地址作为该端口对应的访问控制列表中的 n 个 MAC 地址，n 是访问控制列表允许的最大 MAC 地址数。

(3) 802.1X

一种只允许授权用户使用的终端接入交换机端口的接入控制协议，通常用用户名和口令标识授权用户。

(4) 防 DHCP 欺骗攻击机制

一种通过将交换机端口配置为信任端口和非信任端口，只允许信任端口接收 DHCP 响应消息，以此防止伪造的 DHCP 服务器接入以太网的安全机制。

(5) 防 ARP 欺骗攻击机制

一种通过在交换机中建立所有终端正确的 IP 地址和 MAC 地址对，并以此为依据，阻止包含错误的 IP 地址和 MAC 地址对的 ARP 报文传播的安全机制。

(6) 防源 IP 地址欺骗攻击机制

一种通过在交换机中建立所有终端正确的 IP 地址和 MAC 地址对，并以此为依据，阻止 IP 分组源 IP 地址和封装该 IP 分组的 MAC 帧的源 MAC 地址不匹配的 IP 分组继续传播的安全机制。

(7) 生成树协议

一种通过在交换机之间交换网桥协议数据单元(BPDU)阻塞形成环路的交换机端口，从而使网状以太网成为树形以太网的协议。

(8) 防生成树欺骗攻击机制

一种通过配置使只允许实现交换机互连的交换机端口发送和接收 BPDU，以此阻止黑客终端成为生成树根网桥的安全机制。

第8章 无线局域网安全技术

8.1 例题解析

8.1.1 简答题解析

【例题 8.1】 简述 WEP 的缺陷。

【解析】 一是由于密钥有效期间，所有终端共享 2^{24} 个一次性密钥，因此很容易通过建立一次性密钥字典破译密文；二是一旦黑客获得密钥，即可破译经过无线局域网传输的所有密文；三是身份鉴别机制容易被黑客破解；四是完整性检测机制无法检测出精心设计的篡改。

【例题 8.2】 简述 802.11i 与 802.1X 之间的区别与关系。

【解析】 802.11i 是无线局域网安全协议，由三部分内容组成，分别是加密机制、完整性检测机制和鉴别机制。802.1X 主要实现双向身份鉴别和密钥分配功能，被作为 802.11i 中的身份鉴别机制。

【例题 8.3】 简述 TKIP 在不分段的情况下，发送端封装 MAC 帧的过程和接收端完成完整性检测的过程。

【解析】 发送端与接收端之间已经生成 TK，发送端密钥混合函数的输入是发送端地址 TA、TK 和 TSC，输出是 128 位的 WEP 随机数种子。发送端 michael 函数的输入是 MAC 帧源和目的地址、MAC 帧净荷、MIC 密钥，michael 函数的输出是 MIC。

MAC 帧净荷和 MIC 串接在一起，构成 WEP 数据段，即 WEP 数据段＝MAC 帧净荷 ‖ MIC。根据 WEP 数据段和生成函数 $G(X)$ 计算出 CRC-32，CRC-32 作为 WEP ICV。WEP 伪随机数生成器的输入是 128 位的 WEP 随机数种子，输出是长度等于 WEP 数据段长度＋4 的一次性密钥 K。一次性密钥 K 和 WEP 数据段与 WEP ICV 的串接结果进行异或运算，生成密文(WEP 数据段 ‖ WEP ICV)⊕K。

接收端接收到 TKIP MPDU 后，根据 TKIP MPDU 的发送端地址 TA 找到与 TA 之间的 TK。从 TKIP MPDU 中获取发送端发送的 TSC，以发送端地址 TA、TK 和 TSC 为密钥混合函数的输入，计算出 128 位 WEP 随机数种子。以 128 位 WEP 随机数种子为随机数生成器的输入，计算出长度等于密文的一次性密钥 K，一次性密钥 K 和密文进行异或运算，还原出 WEP 数据段和 WEP ICV，即密文⊕K＝(WEP 数据段 ‖ WEP ICV)⊕K⊕K＝WEP 数据段 ‖ WEP ICV。根据还原出的 WEP 数据段和生成函数 $G(X)$ 计算出 CRC-32，如果计算出的 CRC-32＝还原出的 WEP ICV，接收端通过 WEP 完整性检测。

接收端从 WEP 数据段中分离出 MAC 帧净荷和 MIC，以 TKIP MPDU 中的源和目的地址、WEP 数据段中分离出的 MAC 帧净荷和 MIC 密钥为 michael 函数的输入，计算出 MIC′，如果 MIC′＝WEP 数据段中分离出的 MIC，接收端通过 TKIP 完整性检测。

【例题 8.4】 简述 WEP、WPA 和 WPA-PSK 的差异。

【解析】 WEP 为所有终端和 AP 静态配置相同的密钥，根据是否拥有和 AP 相同的密钥作为判断该终端是否是授权终端的依据，用伪随机数生成函数产生一次性密钥，24 位初始向量和密钥作为随机数种子，所有终端在密钥有效期内共享 2^{24} 个一次性密钥，用循环冗余码作为消息鉴别码。

WPA 为每一个授权用户单独配置身份标识信息，是否能够提供和某个授权用户相同的身份标识信息作为判断该用户是否是授权用户的依据，每一个用户身份鉴别过程中生成独立的 PMK，每一次密钥分配过程生成不同的 TK，每一个终端对应每一个 TK 有着 2^{48} 个一次性密钥，由于 TK 只有终端和 AP 知道，每一个终端只能解密 AP 发送给它的密文。WPA 使用比 WEP 安全性更高的一次性密钥生成算法和消息鉴别码生成算法。

WPA-PSK 和 WPA 不同的是 WPA-PSK 省略了基于用户的身份鉴别过程和 PMK 动态生成过程。所有终端和 AP 静态配置相同的密钥，通过静态配置的密钥导出 PMK，根据是否拥有和 AP 相同的 PMK 作为判断该终端是否是授权终端的依据。由于 TK 计算过程中终端 MAC 地址、AP 和终端选择的随机数都作为输入参数，除非嗅探到密钥分配过程中 AP 和终端交换的两个随机数，否则某个终端无法通过 PMK 推导出另一个终端的 TK。但存在某个终端通过嗅探到另一个终端和 AP 在密钥分配过程中交换的两个随机数，从而推导出另一个终端的 TK 的可能性，这是 WPA-PSK 的一个安全隐患。和 WPA 为不同用户动态生成不同的 PMK 相比，WPA-PSK 的安全性要弱得多。

【例题 8.5】 简述 TKIP 和 CCMP 的差异。

【解析】 一是计算消息鉴别码的算法。TKIP 采用 Michael 算法，CCMP 采用 AES 和加密分组链接模式。二是计算消息鉴别码时，TKIP 除了净荷外，只包括源和目的终端地址，CCMP 包含 MAC 帧首部中所有传输过程中不变的字段。三是一次性密钥计算方法。TKIP 采用伪随机数生成函数，CCMP 采用 AES 和计数器模式。四是 TKIP 使用不同的密钥计算消息鉴别码和一次性密钥，CCMP 用同一个密钥计算消息鉴别码和一次性密钥。

8.1.2 设计题解析

【例题 8.6】 能否通过简单改进 WEP 共享密钥鉴别机制，使黑客终端无法通过嗅探到的特定 IV 和该 IV 对应的一次性密钥，成功完成 AP 对其的身份鉴别过程。

【解析】 黑客终端通过 AP 鉴别的过程如图 8.1 所示，黑客终端通过嗅探获得 AP 发送的 challenge 和授权终端发送的 challenge⊕K 和 IV。由于 challenge⊕K⊕challenge＝K，使黑客终端获取与 challenge 长度相同的一次性密钥 K 和该一次性密钥对应的 IV。

当 AP 鉴别终端身份时，判断终端是否是授权终端的依据是该终端是否拥有与 AP 相同的共享密钥，判断终端是否拥有与 AP 相同的共享密钥的依据是能否生成一个与 challenge 长度相同的一次性密钥，但没有对与该一次性密钥对应的 IV 有任何要求。导

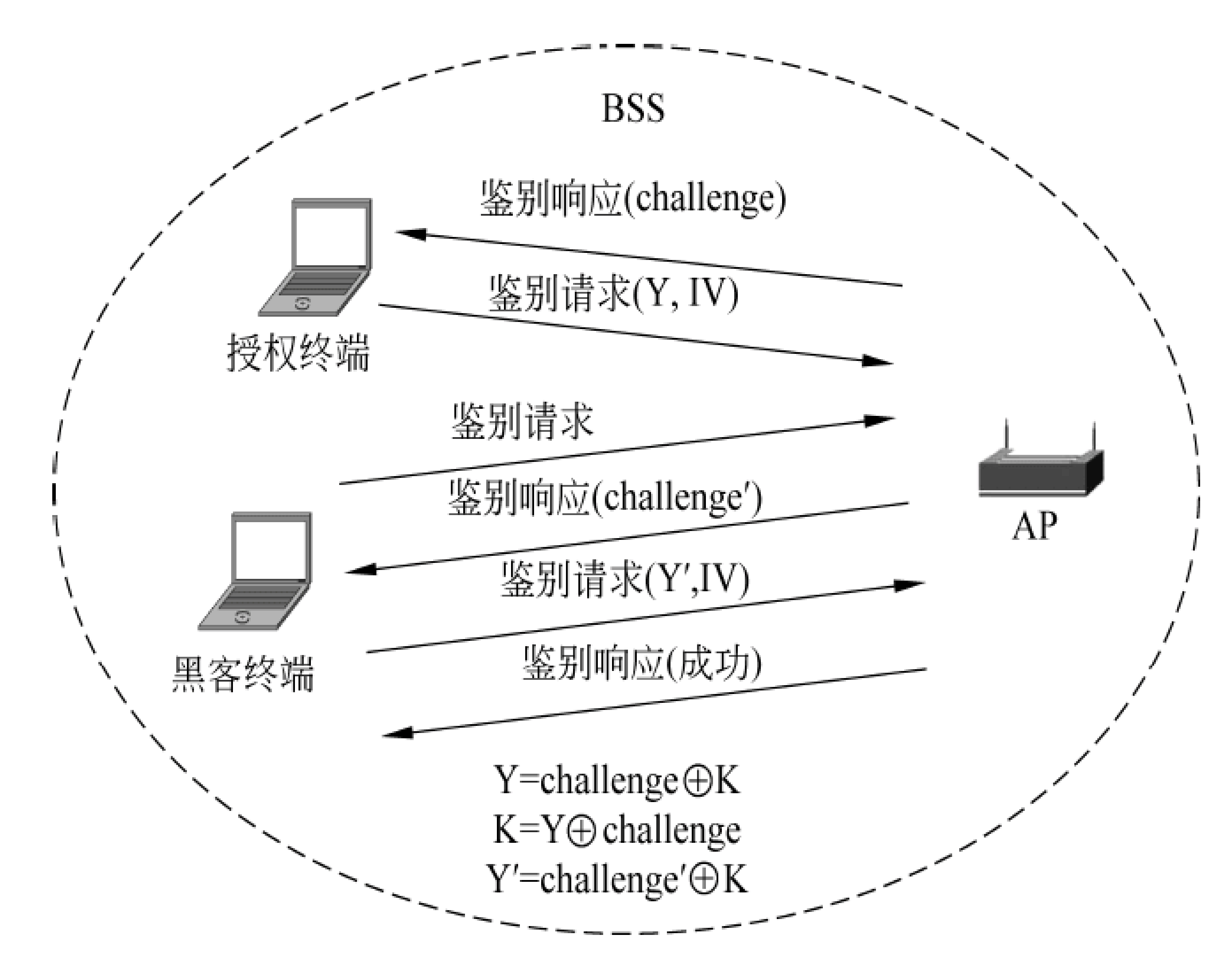


图 8.1　黑客终端通过 AP 鉴别的过程

致黑客终端可以通过经过嗅探获取的与 challenge 长度相同的一次性密钥 K 和该一次性密钥对应的 IV，反复证明自己是授权终端。

改进后的身份鉴别过程如图 8.2 所示，为了鉴别终端身份，AP 向终端同时发送 challenge 和 IV，终端以共享密钥和 AP 发送的 IV 为随机数种子，生成与 challenge 长度相同的一次性密钥 K，计算出密文 Y＝challenge⊕K，并将密文 Y 和 IV 发送给 AP。AP 同样以共享密钥和发送给终端的 IV 作为随机数种子，生成与 challenge 长度相同的一次性密钥 K′。如果 Y⊕K′＝challenge，则表明 K′＝K。终端拥有与 AP 相同的共享密钥。

对于如图 8.2 所示的改进后的身份鉴别过程，即使黑客终端嗅探到 challenge、Y 和 IV，计算出该 IV 对应的一次性密钥 K＝Y⊕challenge。但当黑客终端发起身份鉴别过程时，AP 发送给黑客终端的是 challenge′和 IV′，由于黑客终端无法计算出 IV′对应的一次性密钥 K′，从而无法生成密文 Y′＝challenge′⊕K′。因此无法向 AP 证明拥有与 AP 相同的共享密钥。

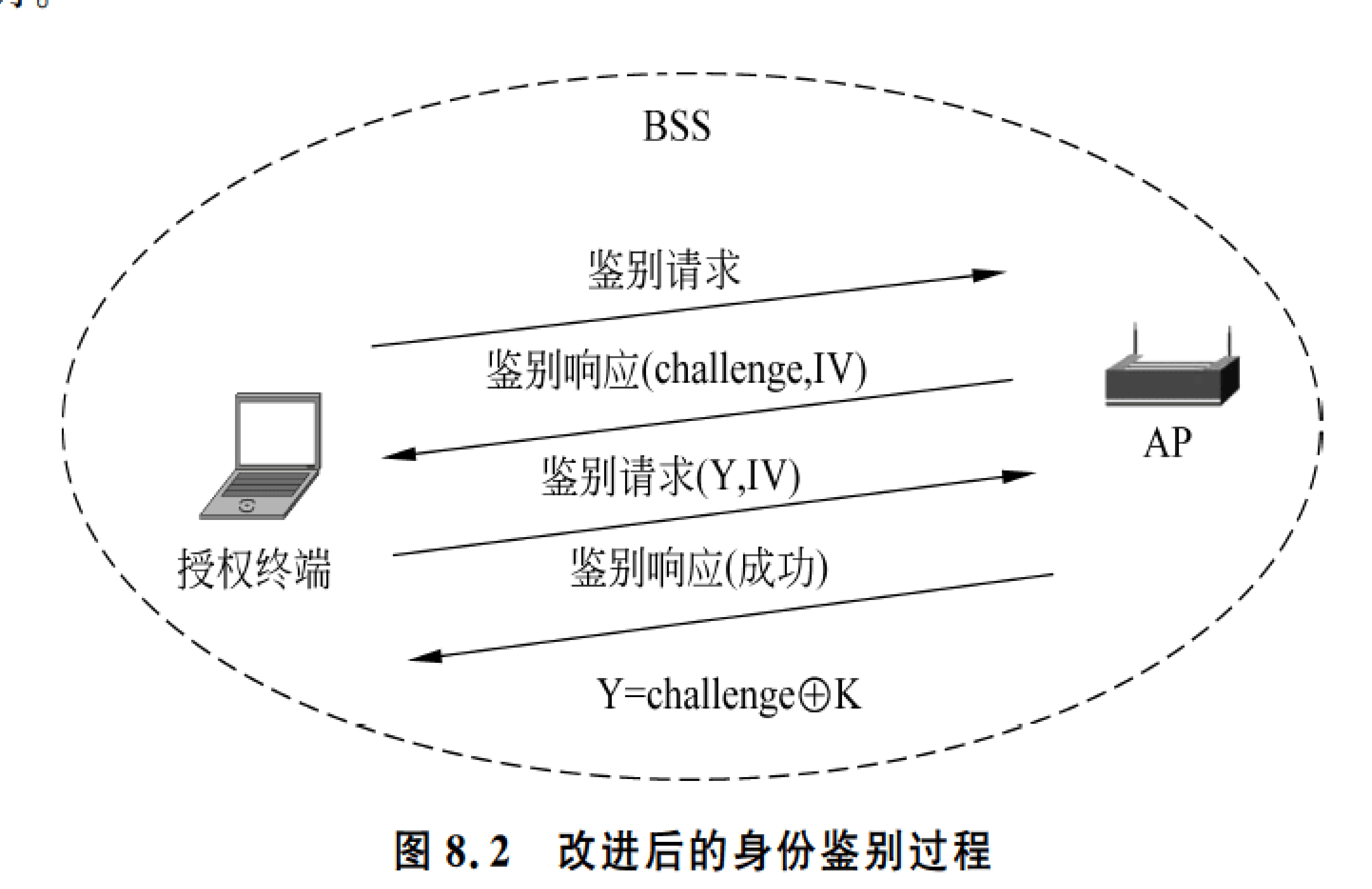


图 8.2　改进后的身份鉴别过程

【例题 8.7】　如果图 8.3 中的无线局域网采用 WEP 安全机制，给出黑客终端非法访问内部网络服务器的全过程。

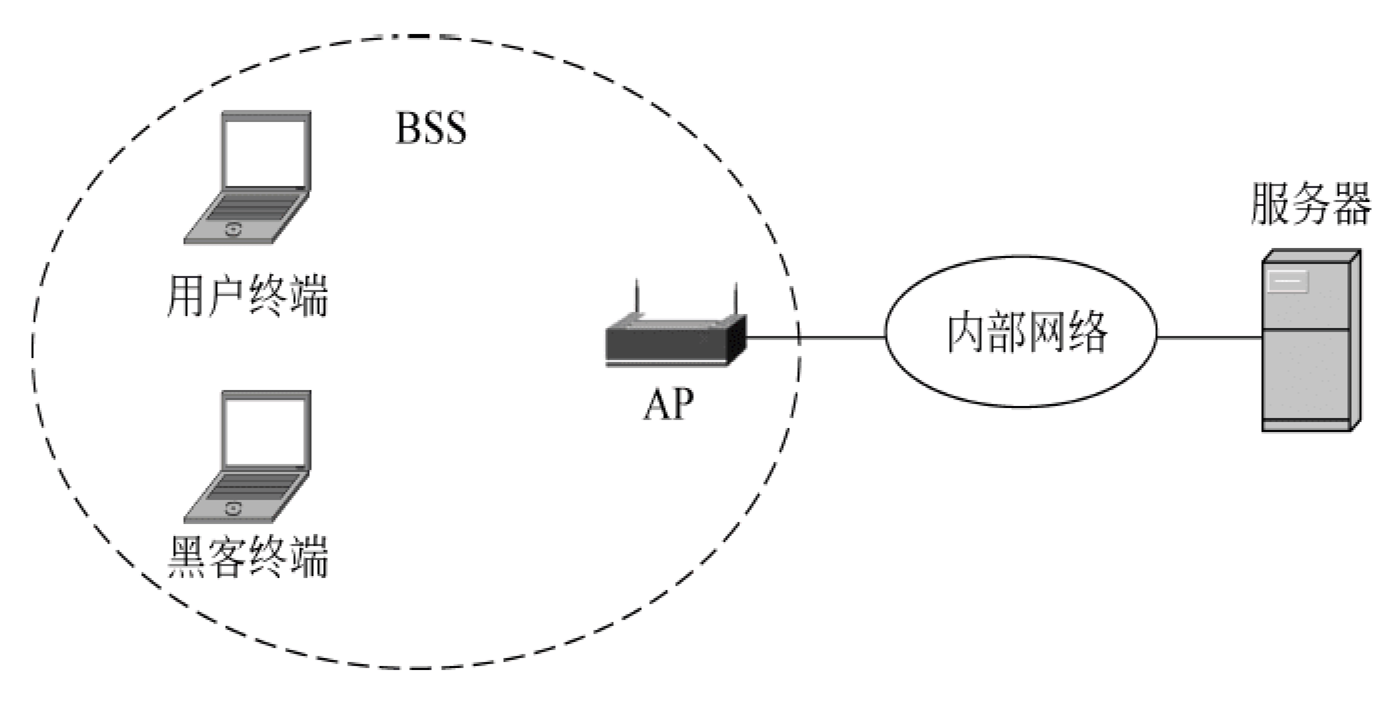


图 8.3　无线接入网络结构

【解析】 如果黑客终端只能嗅探无线局域网中传输的信息，无法接入内部网络，也无法嗅探内部网络中传输的信息，黑客终端要想实现对内部网络服务器的非法访问，只能破解无线局域网中的 WEP 密钥。

当 MAC 帧中净荷是 ARP 报文或者是 IP 分组时，净荷中有些字段的值是固定的，因此，可以根据这些字段的密文导出一次性密钥中这些字段对应的部分。当嗅探到的密文足够多时，有着大量不同的 IV 对应的部分一次性密钥，可以通过分析软件破解 WEP 密钥。

【例题 8.8】 假定存在以下伪 WEP 协议，共享密钥为 4 位，取值 1010。IV 为 2 位，对应 2 位 IV 的 4 种组合的 4 个一次性密钥如下。

101000：0010101101010101001011010100100...

101001：1010011011001010110100100101101...

101010：0001101000111100010100101001111...

101011：1111101010000000101010100010111...

假设所有消息的长度固定为 8 位，ICV 为 4 位，ICV 是消息的前 4 位与后 4 位异或运算结果。伪 WEP 分组包含 3 个字段：IV 字段、消息字段和 ICV 字段，对消息字段和 ICV 字段进行加密。

(1) 如果伪 WEP 协议在 IV=11 的条件下发送消息 m=10100000，求出 WEP 分组 3 个字段的值。

(2) 给出接收端解密该 WEP 分组、完成消息完整性检测的过程。

(3) 如果黑客截获了一个 WEP 分组(IV 值任意)，并在向接收端转发该 WEP 分组前篡改该 WEP 分组，由于黑客不知道共享密钥，因此没有任何 IV 值对应的一次性密钥。假定黑客翻转了 ICV 的第一位，则黑客还须翻转哪些其他位，才能使接收端成功完成完整性检测过程。

【解析】

(1) 由于 8 位消息 m=10100000，因此，ICV=1010⊕0000=1010。WEP 分组中 IV 字段值为 11，消息密文=10100000⊕11111010=01011010。ICV 密文=1010⊕1000=0010，其中 11111010 是 IV=11 时对应的一次性密钥的高 8 位，1000 是 IV=11 时对应的一次性密钥的 9～12 位。

(2) 首先解密消息密文和 ICV 密文，消息=01011010⊕11111010=10100000，ICV=

0010⊕1000=1010。然后重新根据消息计算 ICV′,ICV′=1010⊕0000=1010,由于 ICV′=ICV,接收端成功通过完整性检测。

(3) 假定 8 位消息是 $m_7m_6m_5m_4m_3m_2m_1m_0$,4 为 ICV 是 $c_0c_1c_2c_3$。由于 $c_0=m_7\oplus m_3$,且 $1\oplus c_0=1\oplus m_7\oplus m_3$,因此,在翻转了 ICV 的第一位的情况下,为了保证完整性检测能够通过,或者翻转消息的 m_7,或者翻转消息的 m_3。

【例题 8.9】 图 8.4 展示了一个校园网示意图,如果允许用户任意访问校内网络资源,但必须对用户访问 Internet 的过程进行控制,则应该如何配置无线局域网和鉴别服务器?

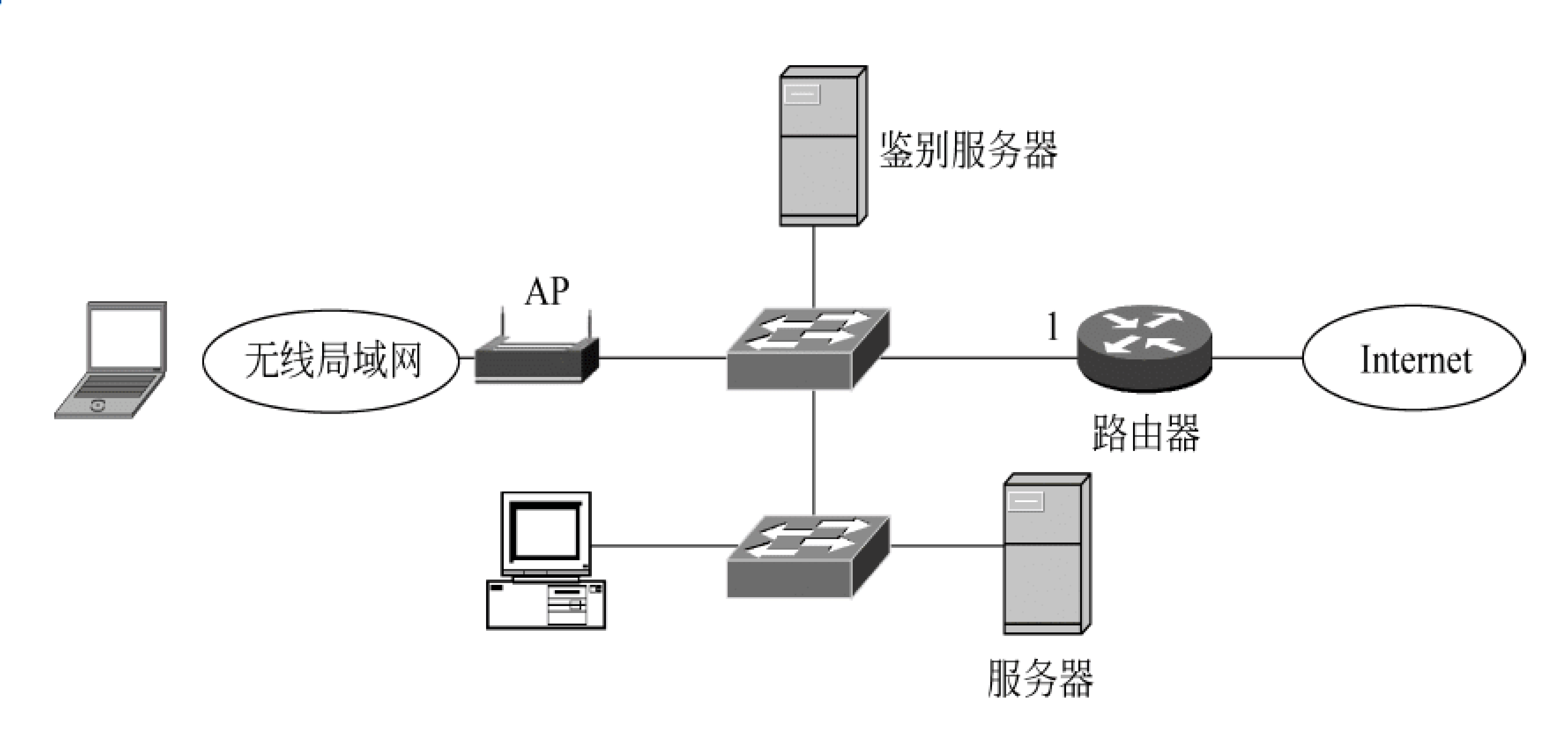


图 8.4 校园网结构

【解析】 因为允许用户任意访问校内网络资源,因此,终端可以任意接入无线局域网和以太网,AP 设置为开放系统鉴别机制。

因为需要限制用户访问 Internet 的过程。因此,路由器接口 1 需要启动 802.1X 接入控制功能,路由器作为鉴别者,需要配置鉴别服务器的 IP 地址及其与鉴别服务器之间的共享密钥。鉴别服务器需要配置授权用户的身份标识信息,如用户名和口令、鉴别者的 IP 地址及与鉴别者之间的共享密钥。鉴别服务器与不同鉴别者之间的共享密钥是不同的。

8.1.3 计算题解析

【例题 8.10】 假定 MAC 帧长度为 200B,无线局域网传输速率为 56Mb/s,求出发送完对应 IV 所有可能组合的 MAC 帧所需的时间(忽略 MAC 帧帧间间隔时间)。

【解析】 发送完对应 IV 所有可能组合的 MAC 帧所需的时间$=2^{24}\times((8\times200)/(56\times10^6))=479.349$s。

【例题 8.11】 在 WEP 安全机制下,假定发送端需要发送的数据是 11011,$G(X)=X^3+X+1$(1011),发送端和接收端使用相同的一次性密钥 11011101,给出篡改者成功实现篡改的过程。

【解析】 由于数据=11011,因此 $M(X)=11011000$,$R(X)=M(X)/G(X)=11011000/1011=001$,即 CRC-3=001。密文=11011 001⊕11011 101=00000 100。

假定用于篡改数据密文的二进制位流=10101,得出 $M1(X)=10101000$,$R1(X)=M1(X)/G(X)=10101000/1011=101$。同时用 10101 篡改数据密文,用 101 篡改 CRC-3 密文,将密文篡改为 00000 100⊕10101 101=10101 001。

接收端根据篡改后的密文还原出的数据和 CRC-3＝10101 001⊕11011 101＝01110 100。其中数据＝01110，CRC-3＝100。由于数据＝01110，因此 $M'(X)$＝01110000，$R'(X)=M'(X)/G(X)$＝01110000/1011＝100。由于计算出的 $R'(X)$与还原后的 CRC-3 相同，接收端认为数据没有被篡改。

8.2 选择题分析

(1) 以下哪一项是无线局域网最大的问题？(　　)

A. 可靠性低　　B. 安全性差

C. 传输速率低　　D. 移动通信能力弱

答案：B

【分析】 无线局域网的开放性导致无线局域网的安全性差。

(2) 以下哪一项是无线局域网开放性带来的安全问题？(　　)

A. 黑客能够轻易接入　　B. 黑客能够轻易嗅探数据

C. 传播的信号易受干扰　　D. A 和 B

答案：D

【分析】 任何能够进入电磁波传播范围且具有指定信道数据接收能力的终端都可嗅探经过无线局域网传输的数据。

(3) 以下哪一项是频段开放性带来的问题？(　　)

A. 方便侦听通信用的电磁波　　B. 方便解密无线传输数据

C. 方便篡改无线传输数据　　D. 方便抵赖无线传输数据

答案：A

【分析】 频段开放性使用于实现无线通信的电磁波频率是公开的，因而很方便侦听用于实现无线通信的电磁波。

(4) 以下哪一项是空间开放性带来的问题？(　　)

A. 方便侦听通信用的电磁波　　B. 方便解密无线传输数据

C. 方便篡改无线传输数据　　D. 方便抵赖无线传输数据

答案：A

【分析】 空间开放性使实现无线通信的电磁波无法局限在某个物理空间内，因而很方便侦听用于实现无线通信的电磁波。

(5) 以下哪一项不是无线局域网容易发生的安全问题？(　　)

A. 嗅探和流量分析　　B. 重放攻击

C. 伪造 AP　　D. ARP 欺骗攻击

答案：D

【分析】 某个终端可以很方便地嗅探同一基本服务区(BSA)中其他终端之间传输的数据，从而可以很方便地实施重放攻击。ARP 欺骗攻击是所有需要建立 IP 地址与 MAC 地址之间绑定关系的传输网络所面临的共同问题，不是无线局域网特有的，也不是无线局域网特别容易发生的。

(6) 以下哪一项不是无线局域网具有的安全功能？(　　)

A. 接入控制　　B. 加密

C. 完整性检测　　D. 数字签名和源端检测

答案：D

【分析】 对于存在 AP 的基本服务集，完成接入控制过程后，AP 主要通过 MAC 帧的源 MAC 地址，或 MAC 帧的目的 MAC 地址确定是否转发该 MAC 帧。

(7) 关于 WEP，以下哪一项描述是错误的？(　　)

A. 用循环冗余码检测数据完整性

B. 伪随机数生成算法作为产生一次性密钥的单向函数

C. 采用流密码体制

D. 一次性密钥不会重复

答案：D

【分析】 由于所有终端共享 2^{24} 个一次性密钥，因此很容易导致一次性密钥重复使用。

(8) 关于 WEP 加密，以下哪一项描述是错误的？(　　)

A. 终端和 AP 必须具有相同的密钥 K

B. 为了同步一次性密钥，发送端需要向接收端发送 IV 明文

C. 黑客无法通过嗅探经过无线网络传输的信息获得密钥 K

D. 黑客无法破译嗅探到的经过无线网络传输的密文

答案：D

【分析】 黑客一旦建立一次性密钥字典，就可以通过 IV 检索出对应的一次性密钥，并用该一次性密钥破译密文。

(9) 关于 WEP 加密机制，以下哪一项描述是错误的？(　　)

A. 共享密钥是授权接入 BSS 的授权标识符

B. 共享密钥长度可以是 40 位或者 104 位

C. 一次性密钥的数量与共享密钥长度无关

D. 一次性密钥的长度等于共享密钥的长度

答案：D

【分析】 一次性密钥长度等于需要加密的明文的长度，与共享密钥长度无关。

(10) 关于 WEP 完整性检测机制，以下哪一项描述是错误的？(　　)

A. ICV 是根据 MAC 帧中数据计算出的 CRC-32

B. 经过无线网络传输的是加密 MAC 帧中数据后生成的数据密文

C. 经过无线网络传输的是加密 ICV 后生成的 ICV 密文

D. 能够检测出对数据密文进行的任何篡改

答案：D

【分析】 假定数据密文是 CD，ICV 密文是 CI，如果进行以下篡改过程：找出一个和数据密文长度相同的数据 M，将数据密文改为 $Y1=CD\oplus M$，将 ICV 密文改为 $Y2=CI\oplus(M/G(X))$，其中 M/G(X) 是根据数据 M 计算出的 CRC-32，则接收端将检测不出已经发

生的篡改。

(11) 关于 WEP 鉴别机制,以下哪一项描述是错误的?( )

A. 共享密钥是授权终端接入的授权标识符

B. AP 通过判断终端能否计算出特定 IV 下的一次性密钥判断终端是否拥有共享密钥

C. 通过嗅探可以获取特定 IV 下的一次性密钥

D. 通过嗅探可以获取共享密钥

答案:D

【分析】 通过嗅探可以获得特定 IV 和该 IV 对应的一次性密钥,但无法根据 IV 和该 IV 对应的一次性密钥导出共享密钥。

(12) 以下哪一项不属于 WEP 的缺陷?( )

A. 所有终端配置相同的密钥

B. 在密钥不变的情况下,只有 2^{24} 个一次性密钥

C. 循环冗余码用于完整性检测

D. 使用流密码体制

答案:D

【分析】 流密码体制本身没有安全缺陷。

(13) 以下哪一项不是建立关联的先决条件?( )

A. AP 与该终端之间完成信道同步过程

B. AP 完成对该终端的身份鉴别过程

C. AP 具有的资源允许该终端接入 BSS

D. AP 的访问控制列表中有该终端的 MAC 地址

答案:D

【分析】 有些厂家的 AP 支持基于 MAC 地址的鉴别机制,即事先将允许接入 BSS 的终端的 MAC 地址配置到 AP 的访问控制列表中,但这种鉴别机制并不是 WEP 的鉴别机制。因此,完成终端身份鉴别过程并不意味着 AP 的访问控制列表中有该终端的 MAC 地址。

(14) 关于 WEP 鉴别机制的缺陷,以下哪一项描述是错误的?( )

A. AP 发送固定长度的 challenge

B. 终端发送的密文 C=challenge⊕一次性密钥 K

C. 黑客终端可以计算出一次性密钥 K=密文 C⊕challenge

D. 黑客终端可以反复通过一次性密钥 K 解密终端发送的数据密文

答案:D

【分析】 每一个不同的 IV 对应着不同的一次性密钥,而且解密数据密文的一次性密钥长度必须等于数据密文的长度。因此,特定 IV 对应的、固定长度的一次性密钥很难用于解密数据密文。

(15) 关于 WEP 加密机制的缺陷,以下哪一项描述是错误的?( )

A. 所有终端共享 2^{24} 个一次性密钥

生的篡改。

(11) 关于 WEP 鉴别机制,以下哪一项描述是错误的?(　　)

A. 共享密钥是授权终端接入的授权标识符

B. AP 通过判断终端能否计算出特定 IV 下的一次性密钥判断终端是否拥有共享密钥

C. 通过嗅探可以获取特定 IV 下的一次性密钥

D. 通过嗅探可以获取共享密钥

答案:D

【分析】 通过嗅探可以获得特定 IV 和该 IV 对应的一次性密钥,但无法根据 IV 和该 IV 对应的一次性密钥导出共享密钥。

(12) 以下哪一项不属于 WEP 的缺陷?(　　)

A. 所有终端配置相同的密钥

B. 在密钥不变的情况下,只有 2^{24} 个一次性密钥

C. 循环冗余码用于完整性检测

D. 使用流密码体制

答案:D

【分析】 流密码体制本身没有安全缺陷。

(13) 以下哪一项不是建立关联的先决条件?(　　)

A. AP 与该终端之间完成信道同步过程

B. AP 完成对该终端的身份鉴别过程

C. AP 具有的资源允许该终端接入 BSS

D. AP 的访问控制列表中有该终端的 MAC 地址

答案:D

【分析】 有些厂家的 AP 支持基于 MAC 地址的鉴别机制,即事先将允许接入 BSS 的终端的 MAC 地址配置到 AP 的访问控制列表中,但这种鉴别机制并不是 WEP 的鉴别机制。因此,完成终端身份鉴别过程并不意味着 AP 的访问控制列表中有该终端的 MAC 地址。

(14) 关于 WEP 鉴别机制的缺陷,以下哪一项描述是错误的?(　　)

A. AP 发送固定长度的 challenge

B. 终端发送的密文 C=challenge⊕一次性密钥 K

C. 黑客终端可以计算出一次性密钥 K=密文 C⊕challenge

D. 黑客终端可以反复通过一次性密钥 K 解密终端发送的数据密文

答案:D

【分析】 每一个不同的 IV 对应着不同的一次性密钥,而且解密数据密文的一次性密钥长度必须等于数据密文的长度。因此,特定 IV 对应的、固定长度的一次性密钥很难用于解密数据密文。

(15) 关于 WEP 加密机制的缺陷,以下哪一项描述是错误的?(　　)

A. 所有终端共享 2^{24} 个一次性密钥

生的篡改。

(11) 关于 WEP 鉴别机制，以下哪一项描述是错误的？(　　)

A. 共享密钥是授权终端接入的授权标识符

B. AP 通过判断终端能否计算出特定 IV 下的一次性密钥判断终端是否拥有共享密钥

C. 通过嗅探可以获取特定 IV 下的一次性密钥

D. 通过嗅探可以获取共享密钥

答案：D

【分析】 通过嗅探可以获得特定 IV 和该 IV 对应的一次性密钥，但无法根据 IV 和该 IV 对应的一次性密钥导出共享密钥。

(12) 以下哪一项不属于 WEP 的缺陷？(　　)

A. 所有终端配置相同的密钥

B. 在密钥不变的情况下，只有 2^{24} 个一次性密钥

C. 循环冗余码用于完整性检测

D. 使用流密码体制

答案：D

【分析】 流密码体制本身没有安全缺陷。

(13) 以下哪一项不是建立关联的先决条件？(　　)

A. AP 与该终端之间完成信道同步过程

B. AP 完成对该终端的身份鉴别过程

C. AP 具有的资源允许该终端接入 BSS

D. AP 的访问控制列表中有该终端的 MAC 地址

答案：D

【分析】 有些厂家的 AP 支持基于 MAC 地址的鉴别机制，即事先将允许接入 BSS 的终端的 MAC 地址配置到 AP 的访问控制列表中，但这种鉴别机制并不是 WEP 的鉴别机制。因此，完成终端身份鉴别过程并不意味着 AP 的访问控制列表中有该终端的 MAC 地址。

(14) 关于 WEP 鉴别机制的缺陷，以下哪一项描述是错误的？(　　)

A. AP 发送固定长度的 challenge

B. 终端发送的密文 C=challenge⊕一次性密钥 K

C. 黑客终端可以计算出一次性密钥 K=密文 C⊕challenge

D. 黑客终端可以反复通过一次性密钥 K 解密终端发送的数据密文

答案：D

【分析】 每一个不同的 IV 对应着不同的一次性密钥，而且解密数据密文的一次性密钥长度必须等于数据密文的长度。因此，特定 IV 对应的、固定长度的一次性密钥很难用于解密数据密文。

(15) 关于 WEP 加密机制的缺陷，以下哪一项描述是错误的？(　　)

A. 所有终端共享 2^{24} 个一次性密钥

B. 共享密钥不变，指定长度的 2^{24} 个一次性密钥不变

C. 容易建立 2^{24} 种 IV 组合与指定长度下的 2^{24} 个一次性密钥之间的对应关系

D. 可以通过 2^{24} 种 IV 组合与指定长度下的 2^{24} 个一次性密钥之间的对应关系导出共享密钥

答案：D

【分析】 随着无线局域网传输速率的提高，发送完 2^{24} 种 IV 组合对应的、有着固定数据长度的 2^{24} 个 MAC 帧所需要的时间越来越短，因此，很容易建立 2^{24} 种 IV 组合与指定长度下的 2^{24} 个一次性密钥之间的对应关系。但无法通过 2^{24} 种 IV 组合与指定长度下的 2^{24} 个一次性密钥之间的对应关系导出共享密钥。

(16) 关于 WEP 完整性检测机制的缺陷，以下哪一项描述是错误的？(　　)

A. ICV 是根据 MAC 帧中数据计算出的 CRC-32

B. 如果 R1 是根据数据 M1 计算出的 CRC-32，R2 是根据数据 M2 计算出的 CRC-32，则 R1⊕R2 是根据数据 M1⊕M2 计算出的 CRC-32

C. 如果 R1 是根据数据 M1 计算出的 CRC-32，且 M1 长度等于数据密文长度，则无法检测出以下篡改：数据密文⊕M1 和 ICV 密文⊕R1

D. 可以将数据明文篡改为任意值

答案：D

【分析】 可以将数据密文篡改为任意值，但在不知道一次性密钥的情况下，无法建立数据明文与数据密文之间的对应关系，因此，无法将数据明文篡改为指定值。

(17) 关于静态密钥管理缺陷，以下哪一项描述是错误的？(　　)

A. 所有终端有着相同的共享密钥

B. 共享密钥不变，指定长度的 2^{24} 个一次性密钥不变

C. 基于终端的接入控制机制

D. 黑客容易猜出共享密钥

答案：D

【分析】 只要配置的共享密钥足够复杂和随机，知道共享密钥的人员不泄露共享密钥，黑客猜出共享密钥是比较困难的。

(18) 关于 802.11i 加密机制，以下哪一项描述是错误的？(　　)

A. 每一个授权接入的用户与 AP 之间有着独立的共享密钥

B. 每一个授权接入的用户与 AP 之间有着 2^{48} 个一次性密钥

C. 授权接入的用户每一次接入时动态生成与 AP 之间的共享密钥

D. 同一授权用户通过不同的终端接入生成相同的与 AP 之间的共享密钥

答案：D

【分析】 在 802.11i 加密机制下，授权用户用不同的终端接入时，生成不同的与 AP 之间的共享密钥。授权用户用同一个终端接入时，每一次接入都生成不同的与 AP 之间的共享密钥。

(19) 关于 802.11i 完整性检测机制，以下哪一项描述是错误的？(　　)

A. 802.11i 的完整性检验值具有单向性

B. 802.11i 的完整性检验值具有抗碰撞性

C. 发送端传输的是加密完整性检验值后生成的消息鉴别码

D. 消息鉴别码是 HMAC-SHA-1-96

答案：D

【分析】 虽然计算 802.11i 完整性检验值的算法具有报文摘要算法的特性，且发送端传输的是加密完整性检验值后生成的消息鉴别码。但 802.11i 生成消息鉴别码的算法不是 HAMC-SHA-1，消息鉴别码的位数也不是 96 位。

(20) 关于 802.11i 身份鉴别机制，以下哪一项描述是错误的？(　　)

A. 基于用户的身份鉴别机制

B. 双向身份鉴别机制

C. 其他终端无法通过嗅探获得鉴别信息

D. 一律用证书＋私钥作为用户和 AP 的身份标识信息

答案：D

【分析】 在一般情况下，用用户名和口令作为用户身份标识信息。由于用户名和口令只有授权用户和鉴别者知道，因此，双方可以通过判别对方是否知道某个授权用户的用户名和口令确定对方身份。当然，前提条件是鉴别过程双方不直接交换用户名和口令。

(21) 关于 TKIP，以下哪一项描述是错误的？(　　)

A. 仍然是流密码体制

B. 采用 Michael 算法计算消息鉴别码

C. 在 TK 不变的情况下，每一个终端拥有 2^{48} 个一次性密钥

D. 如果一些终端的 TK 相同，则这些终端共享 2^{48} 个一次性密钥

答案：D

【分析】 TKIP 计算一次性密钥时，发送端 MAC 地址是其中一个参数，因此，在相同 TK 下，不同的发送端 MAC 地址对应着不同的一次性密钥集。

(22) 关于 TKIP 加密机制，以下哪一项描述是错误的？(　　)

A. 授权用户每一次接入生成不同的与 AP 之间的临时密钥 TK

B. 48 位 TSC 参与一次性密钥计算过程

C. 其他条件不变的情况下，2^{48} 种 TSC 组合对应 2^{48} 个不同的一次性密钥

D. 只有 TK 和 TSC 参与一次性密钥计算过程

答案：D

【分析】 发送端地址 TA、TK 和 TSC 一起参与一次性密钥计算过程。因此，每一个终端有着独立的 2^{48} 个不同的一次性密钥。用户每一次接入有着独立的 2^{48} 个不同的一次性密钥。

(23) 关于 TKIP 加密数据过程，以下哪一项描述是错误的？(　　)

A. 两级密钥混合函数的输入是 TA、TK 和 TSC，输出是 128 位 WEP 随机数种子

B. 128 位 WEP 随机数种子相当于 WEP 的 104 位共享密钥和 24 位 IV

C. 由 WEP 的伪随机数生成器根据 128 位 WEP 随机数种子生成一次性密钥

D. 一次性密钥长度＝MAC帧净荷长度＋MIC长度

答案：D

【分析】 如果没有分段，则数据长度＝MAC帧净荷长度＋MIC长度，则一次性密钥长度＝数据长度＋4。如果分段，则一次性密钥长度＝分段后的数据段长度＋4。长度单位为字节。

(24) 关于TKIP完整性检测机制，以下哪一项描述是错误的？(　　)

A. 计算消息完整性编码的Michael算法具有报文摘要算法的特性

B. 计算消息完整性编码时需要输入MIC密钥

C. 实现完整性检测的内容包括MAC帧净荷、源和目的MAC地址

D. 发送端直接发送消息完整性编码

答案：D

【分析】 消息完整性编码和MAC帧净荷构成数据，对数据用一次性密钥加密后生成密文，发送端发送的是密文。

(25) 关于CCMP加密数据过程，以下哪一项描述是错误的？(　　)

A. 128位AES输入包括48位PN和48位发送端地址

B. 128位AES输出是一次性密钥的一部分

C. TK是AES加密密钥

D. 一次性密钥长度＝数据长度

答案：D

【分析】 CCMP生成的一次性密钥长度等于数据长度＋MIC长度。

(26) 关于CCMP完整性检测过程，以下哪一项描述是错误的？(　　)

A. 将需要完整性检测的信息分段，数据段长度＝128位

B. 采用AES加密算法，TK作为加密密钥

C. 对数据段进行加密分组链接运算

D. 加密分组链接运算的结果是MIC

答案：D

【分析】 加密分组链接运算的结果是最后一级AES的输出，长度为128位。取其高64位和生成的一次性密钥的最高64位进行异或运算，异或运算结果才是MIC。

(27) 关于CCMP，以下哪一项描述是错误的？(　　)

A. 消息鉴别码计算过程中包含MAC帧首部中传输过程中不变的字段

B. 消息鉴别码计算过程中使用AES加密算法和加密分组链接模式

C. 一次性密钥计算过程中使用AES加密算法和计数器模式

D. 使用AES加密算法和加密分组链接模式加密分组后的数据

答案：D

【分析】 一次性密钥计算过程中使用AES加密算法和计数器模式，但仍然通过用一次性密钥和数据的异或操作完成数据加密过程。

(28) 关于802.1X密钥生成过程，以下哪一项描述是错误的？(　　)

A. 如果用用户名和口令作为用户身份标识信息，则通过口令导出PMK

B. 通过 PMK、终端和 AP 的 MAC 地址、终端和 AP 生成的随机数导出 PTK
C. PTK 中至少包含 TK
D. TKIP 和 CCMP 的 PTK 是相同的

答案:D

【分析】 TKIP 和 CCMP 的 PTK 是不同的,因为对于 TKIP,TK 和 MIC 密钥是不同的密钥。对于 CCMP,加密数据和生成 MIC 时使用同一个密钥 TK。

(29) 关于 WPA2 个人模式密钥生成过程,以下哪一项描述是错误的?( )
A. 用户终端和 AP 配置 8~63 个字符长度的密钥
B. 用户终端和 AP 通过配置的密钥导出 256 位 PSK
C. 终端和 AP 直接将 256b 长度的 PSK 作为 PMK
D. WPA2 个人模式只支持 TKIP

答案:D

【分析】 WPA2 个人模式和 802.11i 相比,一是身份鉴别过程不同,二是导出 PMK 的机制不同,加密和完整检测机制是相同的,因此,同时支持 TKIP 和 CCMP 加密和完整性检测机制。CCMP 也称为 AES 加密和完整性检测机制。

(30) 关于 802.11i 的安全性,以下哪一项描述是错误的?( )
A. 不同的授权用户有着不同的与 AP 之间的 TK
B. 任何授权用户无法解密其他授权用户与 AP 之间传输的密文
C. 计算包含 TK 的 PTK 的输入是 PMK、终端和 AP 的 MAC 地址、终端和 AP 生成的随机数
D. 不同授权用户有着不同的 TK 是因为终端的 MAC 地址和终端选择的随机数不同

答案:D

【分析】 因为 PMK 是根据授权用户身份标识信息导出的,因此,不同授权用户导出的 PMK 不同,这是保证任何授权用户无法解密其他授权用户与 AP 之间传输的密文的关键。

(31) 关于 WPA2 个人模式的安全性,以下哪一项描述是错误的?( )
A. 不同终端有着不同的与 AP 之间的 TK
B. 计算包含 TK 的 PTK 的输入是 PMK、终端和 AP 的 MAC 地址、终端和 AP 生成的随机数
C. 任何终端无法解密其他终端与 AP 之间传输的密文
D. 所有授权接入的终端有着相同的 PMK

答案:C

【分析】 由于所有授权接入的终端有着相同的 PMK,当授权接入的终端 X 嗅探到授权接入的终端 Y 与 AP 之间双向身份鉴别过程中相互交换的消息时,可以获取终端 Y 和 AP 的 MAC 地址、终端 Y 和 AP 生成的随机数,从而可以导出终端 Y 与 AP 之间的 TK。因而可以解密终端 Y 与 AP 之间传输的密文。

(32) 以下哪一项不是 WPA2 企业模式优于 WEP 的地方？(　　)

A. 基于用户的接入控制机制

B. 基于用户生成密钥

C. 每一个用户单独拥有 2^{48} 个一次性密钥

D. 使用流密码体制

答案：D

【分析】 差别不是流密码体制，而是一次性密钥生成过程。

(33) 下列哪一项不是 WPA-PSK 优于 WEP 的地方？(　　)

A. 所有终端配置相同的密钥

B. 采用更好的完整性检测算法

C. 每一个终端单独拥有 2^{48} 个一次性密钥

D. 鉴别过程更加安全

答案：A

【分析】 WPA-PSK 同样要求 BSS 中的所有终端静态配置和 AP 相同的密钥。

(34) 以下哪一项描述是错误的？(　　)

A. WEP 在密钥有效期内，所有终端共享 2^{24} 个一次性密钥

B. WPA-PSK 在密钥有效期内，每一个终端单独拥有 2^{48} 个一次性密钥

C. WPA-PSK 根据是否拥有和 AP 相同的密钥判断是否是授权终端

D. WPA 企业模式在安全关联存在期间，每一个用户单独拥有 2^{48} 个一次性密钥

答案：B

【分析】 在 WPA-PSK 下，同一终端每一次密钥分配的过程产生不同的 TK，每个终端对应的每一个 TK 有着 2^{48} 个一次性密钥，在密钥有效期内，可以有无数次的密钥分配过程。

(35) 以下哪一项描述是正确的？(　　)

A. 获取 WEP 密钥能够破译一切经过无线局域网传输的密文

B. 获取 WPA-PSK 密钥能够破译一切经过无线局域网传输的密文

C. 获取 WPA 用户身份标识信息能够破译一切经过无线局域网传输的密文

D. 一旦和 AP 成功建立关联，便能够破译一切经过无线局域网传输的密文

答案：A

【分析】 WEP 计算一次性密钥的参数是密钥 K 和初始向量 IV，初始向量 IV 以明文方式出现在 MAC 帧中，因此，一旦获得密钥 K，则可以计算出对应任何初始向量的一次性密钥。其余三项只能实现和 AP 安全交换数据。

8.3 名词解释

(1) ISM 频段

工业、科学和医疗所使用的电磁波频段，是为了满足公众利用无线电进行通信的需求，允许公众自由使用的开放电磁波频段。

(2) WEP

一种无线局域网安全机制,只能实现 AP 对终端的单向身份鉴别,用 CRC-32 作为完整性检验值,所有终端共享 2^{24} 个一次性密钥。

(3) ICV

在 WEP 安全机制下,根据 MAC 帧净荷和生成函数 G(X)计算出的 CRC-32,用于对 MAC 帧净荷进行完整性检测。

(4) 伪随机数生成器

一种函数模块,可以根据输入的 64 位或 128 位随机数种子,产生任意长度的一次性密钥。

(5) 开放系统鉴别机制

在 WEP 安全机制下,一种允许所有终端接入 BSS 的身份鉴别机制。

(6) 共享密钥鉴别机制

在 WEP 安全机制下,一种通过判断终端能否计算出某个 IV 对应的有效一次性密钥判断终端是否拥有与 AP 相同的共享密钥的身份鉴别机制。

(7) 基于 MAC 地址鉴别机制

一种厂家普遍使用的、只允许 MAC 地址是访问控制列表中的 MAC 地址的终端接入 BSS 的身份鉴别机制。

(8) 一次性密钥字典

一种对应 2^{24} 种 IV 组合,获取指定长度的 2^{24} 个一次性密钥,并通过长度扩展,求出不同长度下 2^{24} 种 IV 组合对应的 2^{24} 个一次性密钥的方法。

(9) 802.11i

一种比 WEP 有着更安全的身份鉴别机制、加密机制和完整性检测机制的无线局域网安全协议。

(10) TKIP

802.11i 中使用的加密和完整性检测协议,不同终端有着不同的与 AP 之间的 TK,每一个 TK 对应 2^{48} 个一次性密钥,通过与报文摘要算法有着相似属性的 Michael 算法计算消息完整性编码。

(11) TK

终端与 AP 之间长度为 128 位的临时密钥,在 TKIP 加密和完整性检测机制下,不同终端有着不同的与 AP 之间的临时密钥。

(12) MIC

在 TKIP 加密和完整性检测机制下,通过 Michael 算法计算出的、用于对 MAC 帧中需要完整性检测的信息进行完整性检测的消息完整性编码。

(13) TSC

在 TKIP 加密和完整性检测机制下,用于产生 48 位参与一次性密钥计算过程的序号的序号计数器,2^{48} 种不同的序号组合对应着 2^{48} 个不同的一次性密钥。

(14) CCMP

802.11i 中使用的加密和完整性检测协议,实现完整性检测时,将需要完整性检测的

信息分割为长度为 128 位的数据段，采用 AES 加密算法，对数据段进行加密分组链接运算，最后一级运算结果中的高 64 位作为完整性检测码。实现加密时，通过 AES 加密算法产生任意长度的一次性密钥，用一次性密钥加密数据和完整性检测码生成密文。

(15) PN

在 CCMP 加密和完整性检测机制下，48 位参与一次性密钥计算过程的报文编号，2^{48} 种不同的报文编号组合对应着 2^{48} 个不同的一次性密钥。

(16) PMK

或者根据终端配置的密钥，或者根据用户身份标识信息导出的 256 位成对主密钥，是计算其他密钥的基础。

(17) PTK

通过 PMK、终端和 AP 的 MAC 地址、终端和 AP 生成的随机数导出的成对过渡密钥，其中包含 TK 和其他密钥。

(18) KCK

包含在 PTK 中，128 位用于对双方进行的密钥产生过程进行证实的证实密钥。

(19) KEK

包含在 PTK 中，128 位用于加密密钥产生过程中传输的机密信息的加密密钥。

(20) MIC 密钥

包含在 PTK 中，在 TKIP 加密和完整性检测机制下，128 位用于生成 MIC 的密钥。

(21) 安全关联

需要进行身份鉴别过程并动态分配临时密钥 TK 的关联。

(22) GMK

AP 通过配置获得的广播主密钥。

(23) GTK

通过 GMK、AP 的 MAC 地址和 AP 生成的随机数导出的临时广播密钥。

(24) WPA2 企业模式

一种由 WiFi 联盟基于 802.11i 标准提出的安全机制，采用基于用户的身份鉴别机制。

(25) WPA2 个人模式

一种由 Wi-Fi 联盟基于 802.11i 标准提出的安全机制，所有终端配置相同的密钥，根据密钥导出 256 位 PMK。由于通过 PMK、终端和 AP 的 MAC 地址、终端和 AP 生成的随机数导出 PTK，因此，不同终端有着不同的与 AP 之间的 TK。

第9章 互连网安全技术

9.1 例题解析

9.1.1 简答题解析

【例题 9.1】 简述 NAT 的安全功能。

【解析】 一是由于分配私有 IP 地址的内部网络对于外部网络是透明的，因此，连接在外部网络上的黑客终端无法对内部网络终端发起主动攻击；二是在建立内部网络私有 IP 地址和全球 IP 地址之间映射前，外部网络终端无法主动和内部网络终端通信，因此，蠕虫病毒很难自动地从外部网络传播到内部网络；三是由于需要通过标准过滤器指定允许进行地址转换的内部网络私有 IP 地址范围，因此，内部网络终端无法通过伪造的不存在的内部网路地址访问外部网络服务器，从而无法对外部网络服务器实施 SYN 泛洪攻击。

9.1.2 设计题解析

【例题 9.2】 互连网结构如图 9.1 所示，给出 RIP 生成的 NET1 至 NET2 的传输路径。如果要求终端 A 与终端 B 之间传输的 IP 分组绕过路由器 R5，给出路由器 R1 配置的策略路由项。

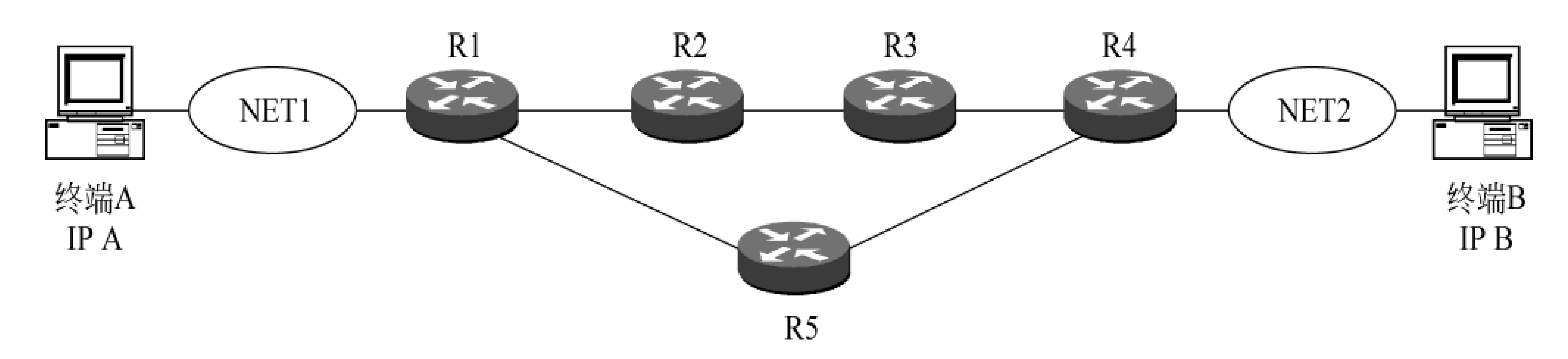


图 9.1 互连网结构

【解析】 路由器 R1 根据 RIP 生成的路由表如图 9.2 所示。

为了绕过路由器 R5，路由器 R1 配置以下策略路由项。

IP 分组分类条件：源 IP 地址＝IP A/32，目的 IP 地址＝IP B/32。

下一跳地址：R2。

类型	目的网络	下一跳	距离
C	NET1	直接	0
R	NET2	R5	2

图 9.2 R1 路由表

【例题 9.3】 在如图 9.3 所示的家庭局域网接

入 Internet 过程中，假定家庭局域网中终端 A 和终端 B 分配的私有 IP 地址分别是 192.168.1.100 和 192.168.1.101，当终端 A 和终端 B 同时访问 Web 服务器时，给出无线路由器地址转换表中可能有的地址转换项。

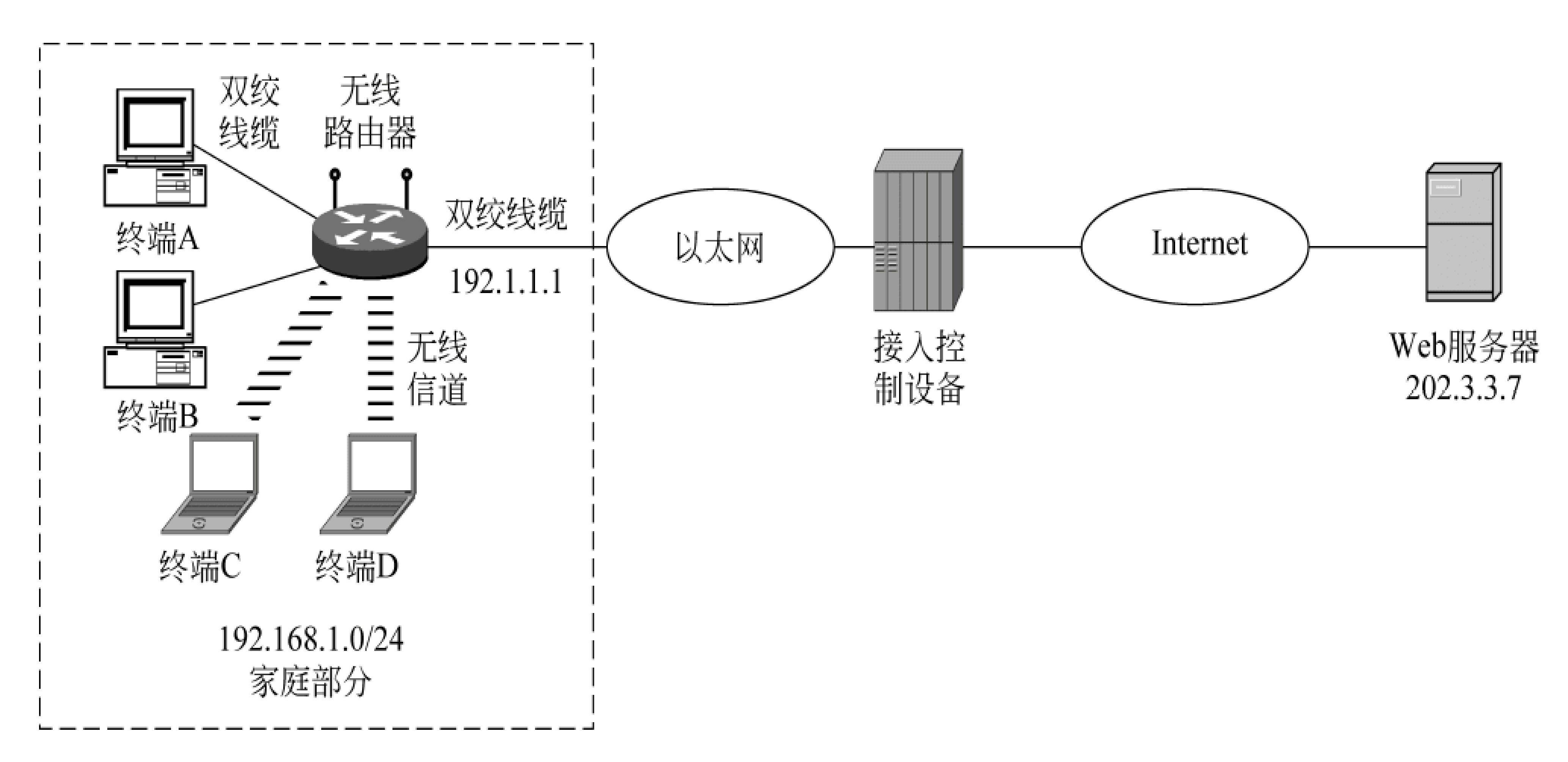


图 9.3　家庭局域网接入 Internet 的结构

【解析】 内部网络终端访问外部网络中的 Web 服务器时，需要用全局唯一的端口号标识内部网络终端，由于源端口号具有本地意义，因此，终端 A 和终端 B 可能选择相同的源端口号，如表 9.1 所示，终端 A 和终端 B 选择相同的源端口号 1024。必须由无线路由器为每一个内部网络终端分配全局唯一的端口号，并建立该全局唯一的端口号与对应的内部网络终端私有 IP 地址之间的映射。因此，在表 9.1 中，用全局唯一的端口号 1024 标识私有 IP 地址为 192.168.1.100 的内部网络终端，用全局唯一的端口号 1025 标识私有 IP 地址为 192.168.1.101 的内部网络终端。

表 9.1　无线路由器地址转换表

协议	Inside Local	Inside Global	Outside Local	Outside Global
TCP	192.168.1.100:1024	192.1.1.1:1024	202.3.3.7:80	202.3.3.7:80
TCP	192.168.1.101:1024	192.1.1.1:1025	202.3.3.7:80	202.3.3.7:80

【例题 9.4】 互连网结构如图 9.4 所示，给出能够实现终端 A 和终端 C 之间相互通信的路由器 R1、R2 的 PAT 配置。

【解析】 由于路由器 R1 和 R2 连接 Internet 的接口只分配一个全球 IP 地址，需要用全局端口号唯一标识内部网络终端。因此，终端 A 和终端 C 之间只能交换 TCP 和 UDP 报文。

路由器 R1 用全局唯一的端口号 8000 标识终端 A，如表 9.2 所示。因此，终端 C 发送的目的 IP 地址为 192.1.1.1，协议类型为 TCP 或 UDP，净荷是目的端口号为 8000 的 TCP 或 UDP 报文的 IP 分组能够到达终端 A。

路由器 R2 用全局唯一的端口号 8000 标识终端 C，如表 9.3 所示。因此，终端 A 发送的目的 IP 地址为 192.1.2.5，协议类型为 TCP 或 UDP，净荷是目的端口号为 8000 的

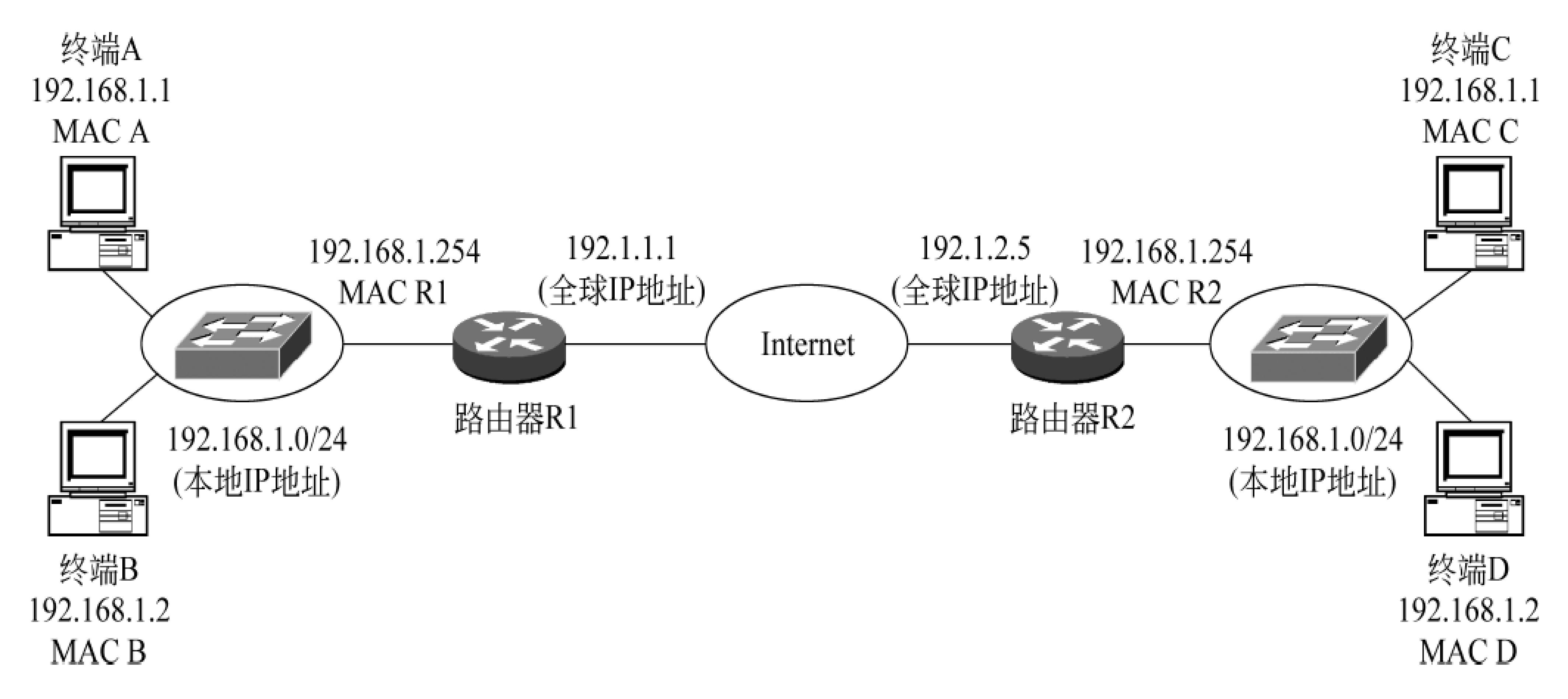


图 9.4　互连网结构

TCP 或 UDP 报文的 IP 分组能够到达终端 C。

表 9.2　R1 地址转换表

协议	Inside Local	Inside Global
TCP	192.168.1.1:8000	192.1.1.1:8000
UDP	192.168.1.1:8000	192.1.1.1:8000

表 9.3　R2 地址转换表

协议	Inside Local	Inside Global
TCP	192.168.1.1:8000	192.1.2.5:8000
UDP	192.168.1.1:8000	192.1.2.5:8000

【例题 9.5】 对应如图 9.5 所示的互连网结构和 IP 地址配置，给出能够实现终端 A 与 Web 服务器 2、终端 B 与 Web 服务器 1 之间相互通信的配置(包括路由器 R1、R2 的路

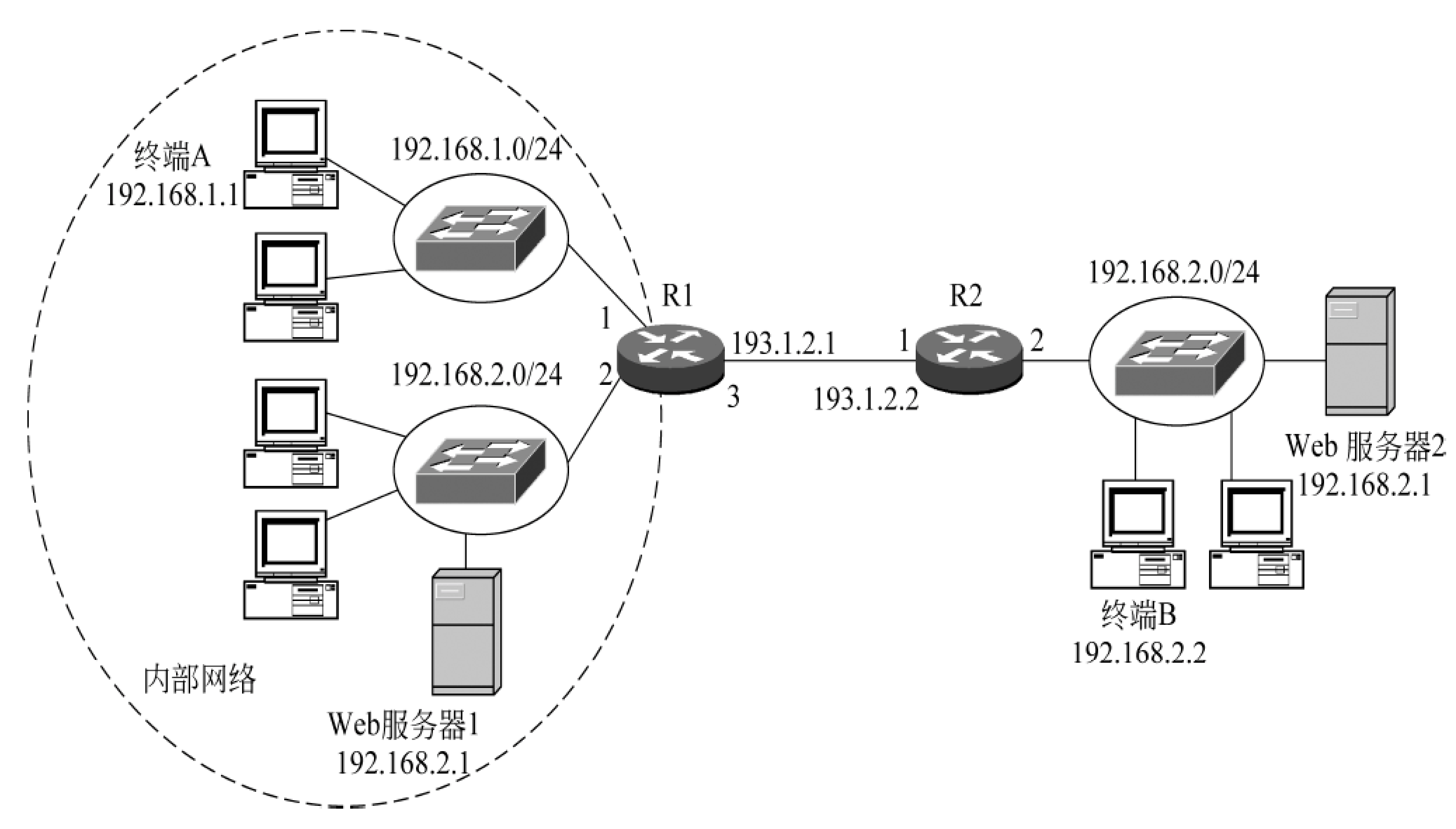


图 9.5　互连网结构

由表和 PAT 配置)。

【解析】 路由器 R1 路由表中需要给出用于指明通往内部网络各个子网和路由器 R2 连接公共网络的接口的传输路径的路由项,如表 9.4 所示。路由器 R2 路由表中需要给出用于指明通往内部网络和路由器 R1 连接公共网络的接口的传输路径的路由项,如表 9.5 所示。

路由器 R1 用全局唯一的端口号 80 标识 Web 服务器 1,如表 9.6 所示,因此,终端 B 可以通过 URL=193.1.2.1 访问 Web 服务器 1。同样,路由器 R2 用全局唯一的端口号 80 标识 Web 服务器 2,如表 9.7 所示,因此,终端 A 可以通过 URL=193.1.2.2 访问 Web 服务器 2。

表 9.4　R1 路由表

目的网络	子网掩码	下一跳	输出接口
192.168.1.0	255.255.255.0	直接	1
192.168.2.0	255.255.255.0	直接	2
193.1.2.0	255.255.255.0	直接	3

表 9.5　R2 路由表

目的网络	子网掩码	下一跳	输出接口
192.168.2.0	255.255.255.0	直接	2
193.1.2.0	255.255.255.0	直接	1

表 9.6　R1 地址转换表

协　议	Inside Local	Inside Global
TCP	192.168.2.1:80	193.1.2.1:80

表 9.7　R2 地址转换表

协　议	Inside Local	Inside Global
TCP	192.168.2.1:80	193.1.2.2:80

【例题 9.6】 对应如图 9.6 所示的互连网结构和 IP 地址配置,给出能够实现内部网

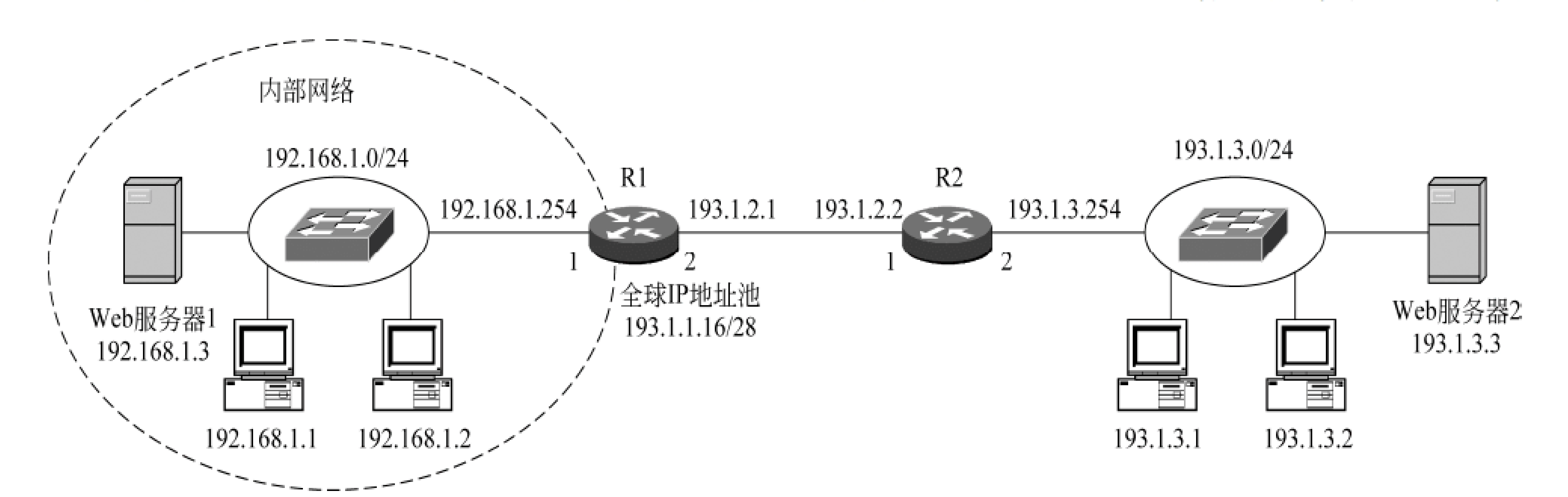


图 9.6　互连网结构

络终端访问 Web 服务器 2、外部网络终端访问 Web 服务器 1 所需要的配置(包括路由器路由表和路由器 R1 的 NAT 配置)。

【解析】 路由器 R1 路由表中需要给出用于指明通往内部网络和外部网络各个子网的传输路径的路由项,如表 9.8 所示。路由器 R2 路由表中只给出用于指明通往外部网络各个子网的传输路径的路由项,如表 9.9 所示。

对于 NAT,为了允许外部网络终端访问内部网络的 Web 服务器 1,需要事先建立 Web 服务器 1 的私有 IP 地址 192.168.1.3 与全球 IP 地址 193.1.1.30 之间的映射,如表 9.10 所示,建立映射后,外部网络终端可以用全球 IP 地址 193.1.1.30 访问 Web 服务器 1。

内部网络终端为了能够访问 Web 服务器 2,需要动态建立私有 IP 地址与全球 IP 地址之间的映射,如表 9.10 所示的私有 IP 地址 192.168.1.1 与全球 IP 地址 193.1.1.17 之间的映射。

值得强调的是,建立私有 IP 地址与全球 IP 地址之间的映射后,外部网络终端可以通过该全球 IP 地址向该全球 IP 地址对应的内部网络终端发送任何净荷类型的 IP 分组。

表 9.8 R1 路由表

目的网络	子网掩码	下一跳	输出接口
192.168.1.0	255.255.255.0	直接	1
193.1.2.0	255.255.255.0	直接	2
193.1.3.0	255.255.255.0	193.1.2.2	2

表 9.9 R2 路由表

目的网络	子网掩码	下一跳	输出接口
193.1.2.0	255.255.255.0	直接	1
193.1.3.0	255.255.255.0	直接	2

表 9.10 R1 地址转换表

协议	Inside Local	Inside Global
IP	192.168.1.3	193.1.1.30
IP	192.168.1.1	193.1.1.17

【例题 9.7】 假定一个企业需要将两个内部网络通过无线路由器接入 Internet。完成连接过程和终端网络信息配置过程。

【解析】 无线路由器是一种比较特殊的设备,一方面具有互连内部网络与外部网络、实现内部网络终端访问外部网络资源的功能。另一方面,内部网络终端对外部网络是不可见的,对于外部网络中的其他路由器和终端,无线路由器等同于一个接入外部网络的终端。因此,如果需要将两个内部网络接入 Internet,采用如图 9.7 所示的连接方式,无线路由器 R2 互连 Internet 和内部网络 1,LAN 端口分配属于内部网络 1 的 IP 地址,WAN

端口分配 Internet 全球 IP 地址。无线路由器 R1 互连内部网络 1 和内部网络 2，LAN 端口分配属于内部网络 2 的 IP 地址，WAN 端口分配属于内部网络 1 的 IP 地址。对于 Internet 中的终端和路由器，内部网络 1 和内部网络 2 都是不可见的，图 9.7 中的 Web 服务器发送给内部网络 1 和内部网络 2 的 IP 分组都是以路由器 R2 连接 Internet 的端口(WAN 端口)的 IP 地址为目的 IP 地址。同样，对于内部网络 1 中的终端，内部网络 2 也是不可见的，如图 9.7 所示的终端 B 发送给内部网络 2 的 IP 分组是以路由器 R1 连接内部网络 1 的端口(WAN 端口)的 IP 地址为目的 IP 地址。

在图 9.7 展示的接入网络中，内部网络 1 和内部网络 2 中的终端可以发起访问 Internet 的过程。内部网络 2 中的终端可以发起访问内部网络 1 的过程，但 Internet 中的终端不能发起访问内部网络 1 和内部网络 2 的过程，内部网络 1 中的终端不能发起访问内部网络 2 的过程。

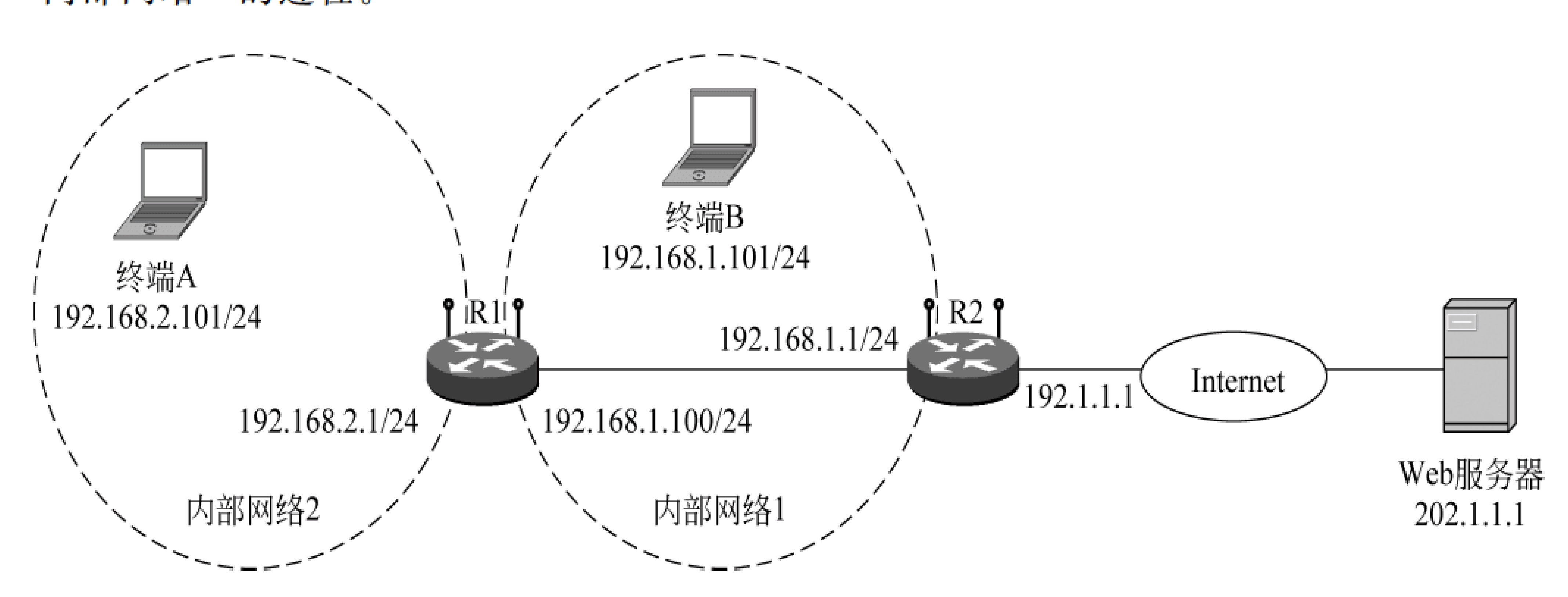


图 9.7 两个内部网络接入 Internet 的过程

【例题 9.8】 如图 9.8 所示，终端 A 发起访问终端 B 的过程交换图中编号为①～④的 IP 分组，IP 分组的传输顺序与编号一致。终端 A 发起访问 Web 服务器的过程交换图中编号为⑤～⑩的 IP 分组，IP 分组的传输顺序与编号一致。给出这些 IP 分组的源和目的 IP 地址。

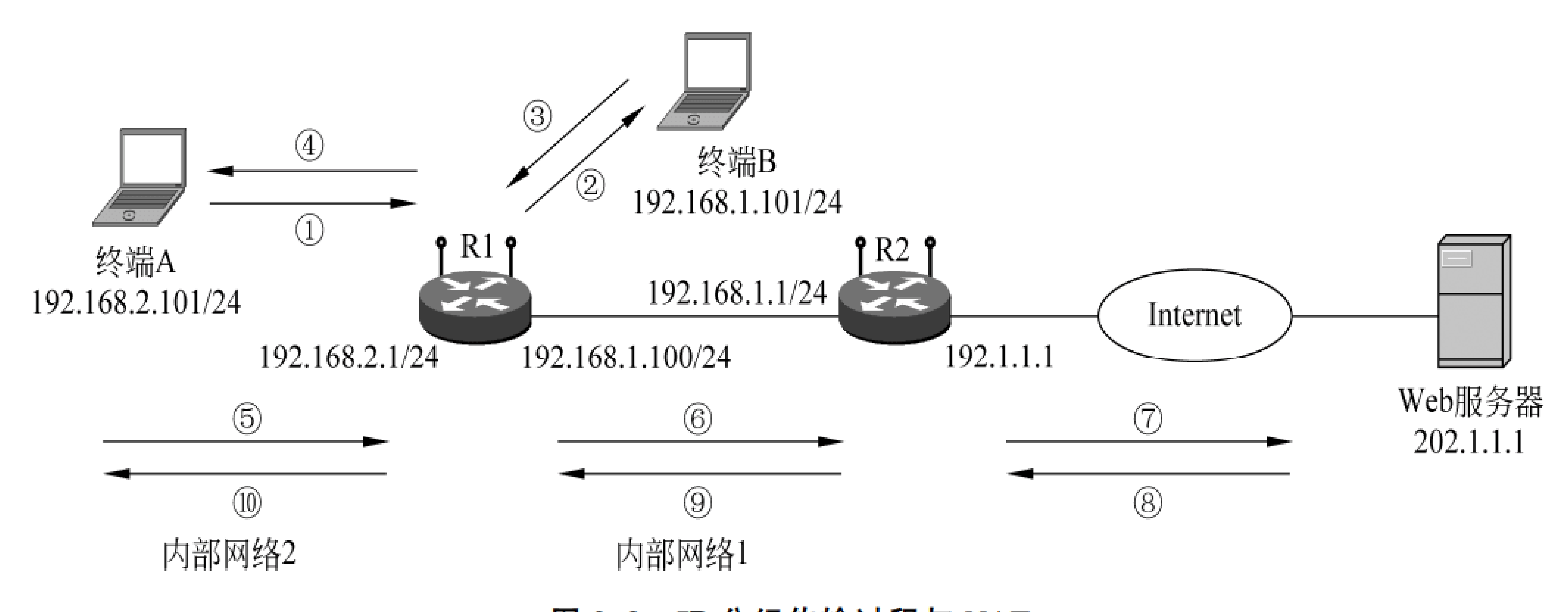


图 9.8 IP 分组传输过程与 NAT

【解析】 如表 9.11 所示，编号①的 IP 分组是终端 A 传输给终端 B，且在内部网络 2 内传输的 IP 分组，该 IP 分组的目的 IP 地址是终端 B 的 IP 地址，源 IP 地址是终端 A 的 IP 地址。编号②的 IP 分组是终端 A 传输给终端 B，且在内部网络 1 内传输的 IP 分组，

由于终端 A 对于内部网络 1 是不可见的，因此，该 IP 分组的源 IP 地址转换为分配给无线路由器 R1 的 WAN 端口的属于内部网络 1 的 IP 地址 192.168.1.100。IP 分组的目的 IP 地址是终端 B 的 IP 地址。

表 9.11 IP 分组源和目的 IP 地址

编　　号	源 IP 地址	目的 IP 地址
①	192.168.2.101	192.168.1.101
②	192.168.1.100	192.168.1.101
③	192.168.1.101	192.168.1.100
④	192.168.1.101	192.168.2.101
⑤	192.168.2.101	202.1.1.1
⑥	192.168.1.100	202.1.1.1
⑦	192.1.1.1	202.1.1.1
⑧	202.1.1.1	192.1.1.1
⑨	202.1.1.1	192.168.1.100
⑩	202.1.1.1	192.168.2.101

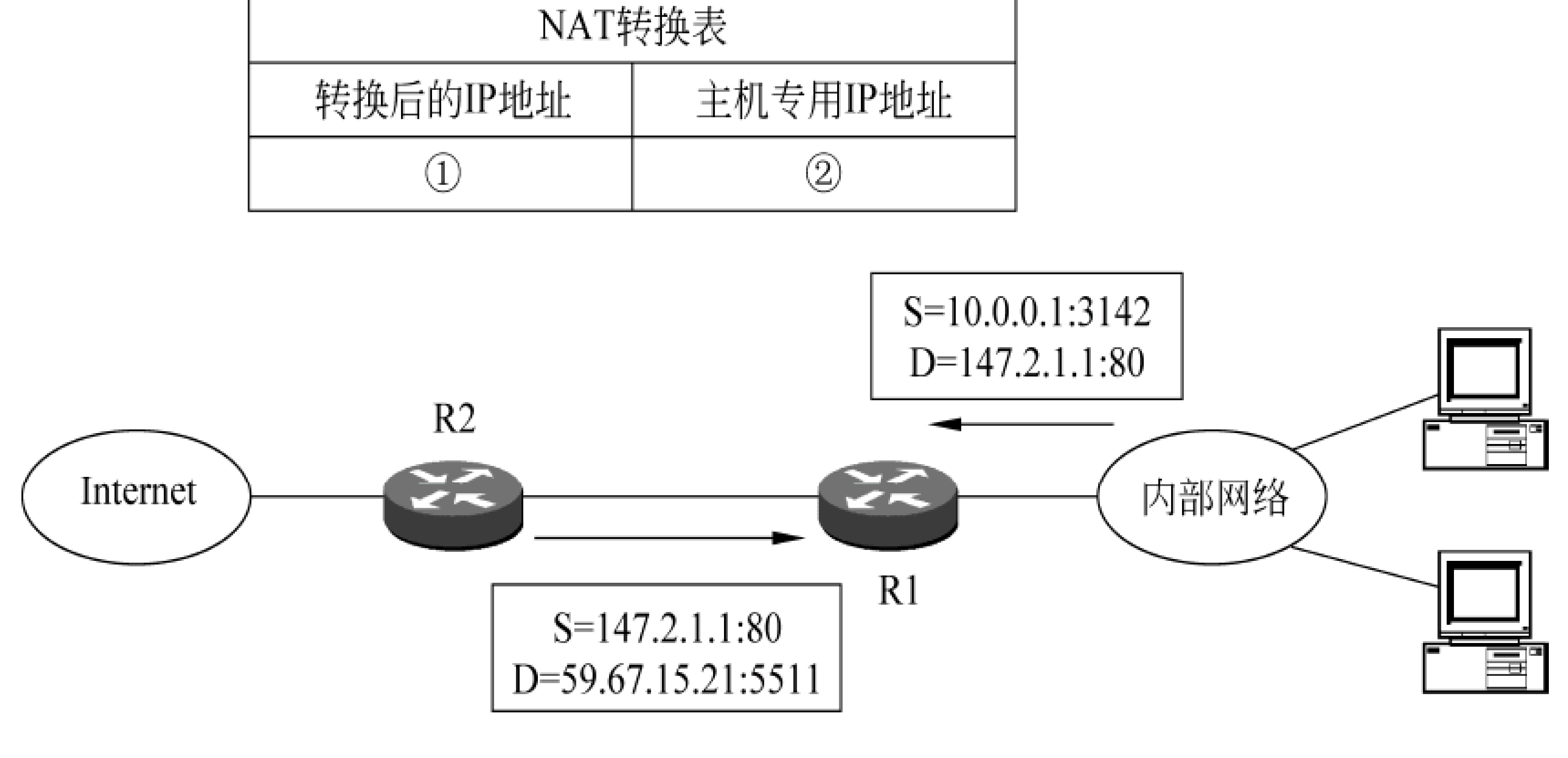
编号③的 IP 分组是终端 B 传输给终端 A，且在内部网络 1 内传输的 IP 分组，由于终端 A 对于内部网络 1 是不可见的，因此，该 IP 分组的目的 IP 地址是分配给无线路由器 R1 的 WAN 端口的属于内部网络 1 的 IP 地址 192.168.1.100。IP 分组的源 IP 地址是终端 B 的 IP 地址。编号④的 IP 分组是终端 B 传输给终端 A，且在内部网络 2 内传输的 IP 分组，该 IP 分组的目的 IP 地址是终端 A 的 IP 地址，源 IP 地址是终端 B 的 IP 地址。

编号⑤的 IP 分组是终端 A 传输给 Web 服务器，且在内部网络 2 内传输的 IP 分组，该 IP 分组的目的 IP 地址是 Web 服务器的 IP 地址，源 IP 地址是终端 A 的 IP 地址。编号⑥的 IP 分组是终端 A 传输给 Web 服务器，且在内部网络 1 内传输的 IP 分组，由于终端 A 对于内部网络 1 是不可见的，因此，该 IP 分组的源 IP 地址转换为分配给无线路由器 R1 的 WAN 端口的属于内部网络 1 的 IP 地址 192.168.1.100。IP 分组的目的 IP 地址是 Web 服务器的 IP 地址。编号⑦的 IP 分组是终端 A 传输给 Web 服务器，且在 Internet 内传输的 IP 分组，由于内部网络 1 和内部网络 2 对于 Internet 都是不可见的，因此，该 IP 分组的源 IP 地址转换为分配给无线路由器 R2 的 WAN 端口的全球 IP 地址 192.1.1.1。IP 分组的目的 IP 地址是 Web 服务器的 IP 地址。

编号⑧的 IP 分组是 Web 服务器传输给终端 A，且在 Internet 内传输的 IP 分组，由于内部网络 1 和内部网络 2 对于 Internet 都是不可见的，因此，该 IP 分组的目的 IP 地址是分配给无线路由器 R2 的 WAN 端口的全球 IP 地址 192.1.1.1。IP 分组的源 IP 地址是 Web 服务器的 IP 地址。编号⑨的 IP 分组是 Web 服务器传输给终端 A，且在内部网

络 1 内传输的 IP 分组，由于内部网络 2 对于内部网络 1 是不可见的，因此，该 IP 分组的目的 IP 地址是分配给无线路由器 R1 的 WAN 端口的属于内部网络 1 的 IP 地址 192.168.1.100。IP 分组的源 IP 地址是 Web 服务器的 IP 地址。编号⑩的 IP 分组是 Web 服务器传输给终端 A，且在内部网络 2 内传输的 IP 分组，该 IP 分组的目的 IP 地址是终端 A 的 IP 地址，源 IP 地址是 Web 服务器的 IP 地址。

【例题 9.9】 如图 9.9 所示是网络地址转换（NAT）的一个示例，路由器 R1 互连内部网络和外部网络，具有 NAT 功能，分析得出图 9.9 中①和②的值。



NAT转换表	
转换后的IP地址	主机专用IP地址
①	②

图 9.9　NAT 示例

【解析】 由于内部网络终端传输给外部网络，且在内部网络内传输的 IP 分组的源 IP 地址是内部网络终端的私有 IP 地址，目的 IP 地址是外部网络终端的全球 IP 地址。因此，通过内部网络终端传输给路由器 R1 的 IP 分组可以发现，内部网络终端的 IP 地址是 10.0.0.1，源端口号是 3142。由于外部网络终端传输给内部网络，且在外部网络内传输的 IP 分组的目的 IP 地址是路由器 R1 连接外部网络的接口的全球 IP 地址。因此，通过 Internet 传输给路由器 R1 的 IP 分组可以发现，路由器 R1 连接外部网络的接口的 IP 地址是 59.67.15.21，目的端口号是 5511。

NAT 转换表中某项转换项的主机专用 IP 地址是内部网络终端的私有 IP 地址和内部网络终端选择的源端口号，因此主机专用 IP 地址是 10.0.0.1 和 3142。转换后的 IP 地址是路由器 R1 连接外部网络的接口的 IP 地址和路由器 R1 选择的源端口号，而路由器 R1 选择的源端口号成为外部网络发送给路由器 R1 的报文的目的端口号，因此，转换后的 IP 地址是 59.67.15.21 和 5511。求出①是 59.67.15.21 和 5511，②是 10.0.0.1 和 3142。

【例题 9.10】 对于如图 9.10 所示的互连网结构，如果要求连接在网络 192.1.1.0/24 和 192.1.2.0/24 的终端各有一半以路由器 R1 和 R2 作为默认网关，给出实现这一功能所需的 VRRP 配置。

【解析】 如图 9.11 所示，创建 VRID 分别为 2 和 3 的两个虚拟路由器，并将路由器 R1 接口 1 和路由器 R2 接口 1 分配给 VRID 为 2 和 3 的两个虚拟路由器，为 VRID 为 2 的虚拟路由器分配虚拟 IP 地址 192.1.1.253，使路由器 R2 成为 VRID 为 2 的虚拟路由器的主路由器，为 VRID 为 3 的虚拟路由器分配虚拟 IP 地址 192.1.1.254，使路由器 R1

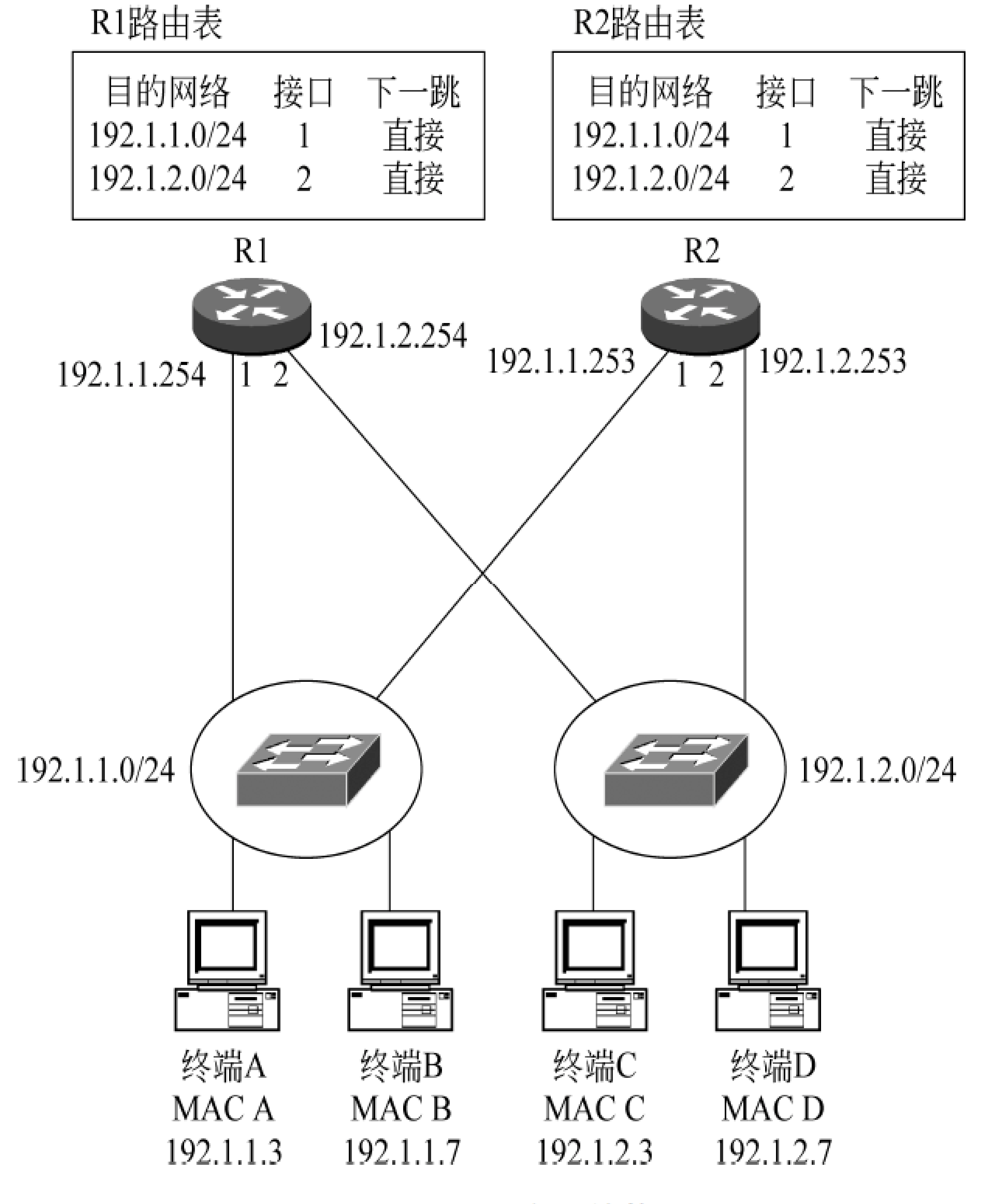


图 9.10 互连网结构

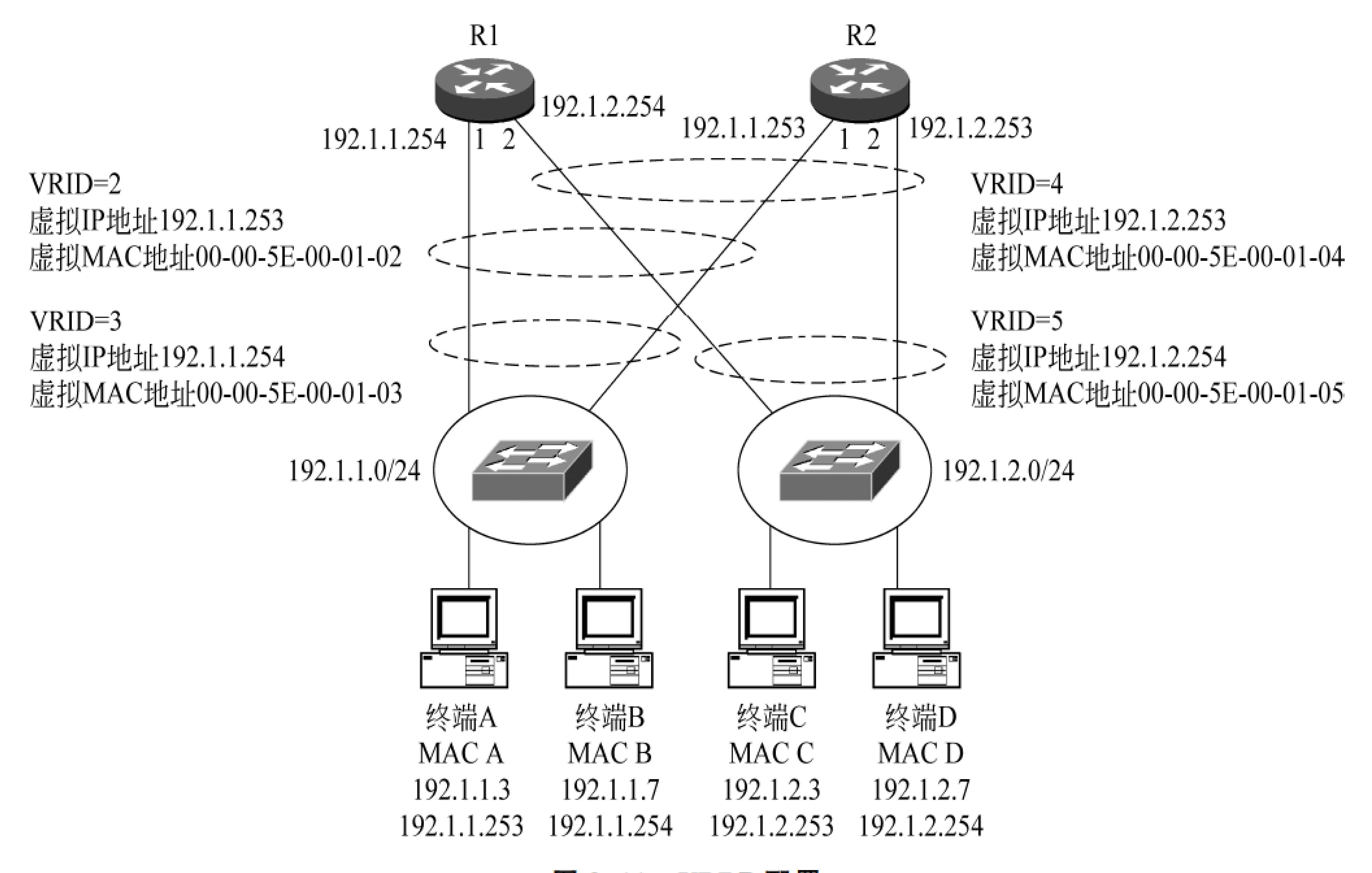


图 9.11 VRRP 配置

成为 VRID 为 3 的虚拟路由器的主路由器。

如图 9.11 所示，创建 VRID 分别为 4 和 5 的两个虚拟路由器，并将路由器 R1 接口 2 和路由器 R2 接口 2 分配给 VRID 为 4 和 5 的两个虚拟路由器，为 VRID 为 4 的虚拟路由

器分配虚拟 IP 地址 192.1.2.253，使路由器 R2 成为 VRID 为 4 的虚拟路由器的主路由器，为 VRID 为 5 的虚拟路由器分配虚拟 IP 地址 192.1.2.254，使路由器 R1 成为 VRID 为 5 的虚拟路由器的主路由器。

如图 9.11 所示，终端 A 的默认网关地址为虚拟 IP 地址 192.1.1.253、终端 B 的默认网关地址为虚拟 IP 地址 192.1.1.254。终端 C 的默认网关地址为虚拟 IP 地址 192.1.2.253、终端 D 的默认网关地址为虚拟 IP 地址 192.1.2.254。

9.1.3 计算题解析

【例题 9.11】 假定漏斗算法中的队列长度是 10MB，队列稳定器的输出速率是 2Mb/s，求分组最大队列等待时延。

【解析】 分组最大队列等待时延 $=(10\times10^6\times8)/(2\times10^6)=40s$。

【例题 9.12】 假定每一个令牌授权传输 2KB，令牌生成速率是 1000 个/s。令牌桶深度是 1000 个令牌，求平均传输速率和最大突发性数据长度。

【解析】 平均传输速率＝每一个令牌授权传输的二进制数位数×令牌生成速率＝$2\times10^3\times8\times1000=16Mb/s$。

最大突发性数据长度＝每一个令牌授权传输的二进制数位数×令牌桶深度＝$2\times10^3\times8\times1000=16Mb=2MB$。

【例题 9.13】 网络结构如图 9.12 所示，假定 IP 首部长度为 20B，回答以下问题。

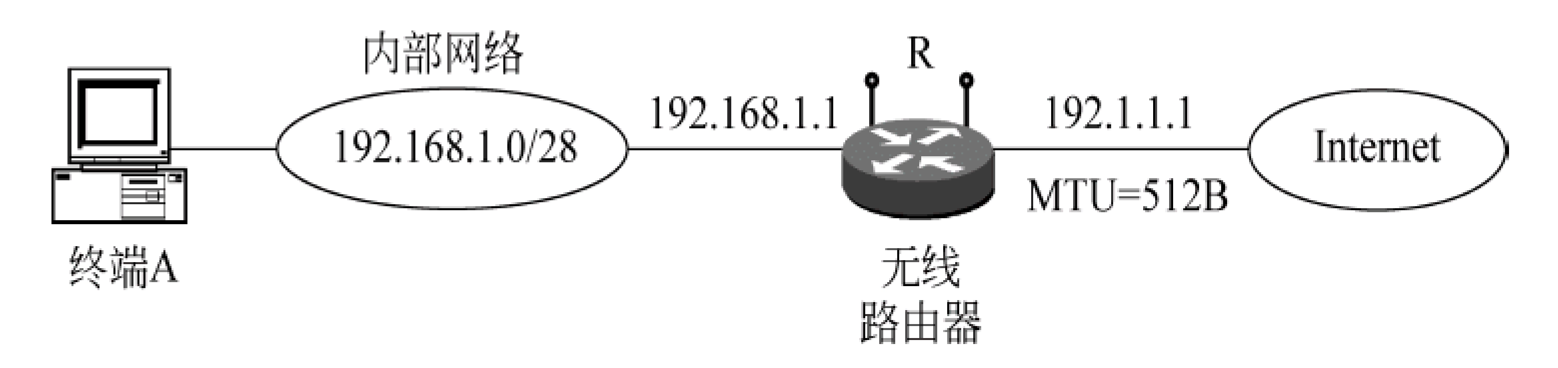


图 9.12　网络结构

(1) 终端 A 配置网络信息时，正确的子网掩码和默认网关地址分别是多少？

(2) 如果由路由器 R 向互连网转发一个源 IP 地址＝192.168.1.5、ID＝12345、length＝500B、DF＝1 的 IP 分组，该 IP 分组首部的哪些字段会被修改？如何修改？

(3) 如果由路由器 R 向互连网转发一个源 IP 地址＝192.168.1.10、ID＝6789、length＝1500B、DF＝0 的 IP 分组，路由器需要将该 IP 分组分为几片(每片尽可能封装为最大片)？求出封装每片数据片的 IP 分组首部的 ID、DF、MF、length、offset 的值。

【解析】

(1) 无线路由器 R 连接内部网络的接口的 IP 地址就是终端 A 的默认网关地址，因此，终端 A 的默认网关地址是 192.168.1.1。由于分配给内部网络的网络地址的网络号位数＝28，因此，子网掩码是 255.255.255.240。

(2) 由于 IP 分组总长为 500B，小于无线路由器 R 连接 Internet 链路的 MTU，因此，无线路由器 R 在完成内部网络至 Internet 的 IP 分组转发过程中，一是需要修改源 IP 地址字段，将源 IP 地址由 192.168.1.5 改为 192.1.1.1；二是需要修改 TTL 字段值，将 TTL 字段值减 1；三是需要重新计算检验和。

(3) IP 分组的数据长度=1500−20=1480。因此,数据片数 n 满足不等式 $n\times512\geq1480+20\times n$ 的最小 n 值,求出 $n=4$。前三片数据片的长度 L 是满足以下条件的最大 L,一是 $L+20\leq512$,二是 L 是 8 的倍数,求出 $L=488$。第 4 片数据片长度=1480−3×488=16。以此得出封装第 1 片数据片的 IP 分组首部的 offset(片偏移)=0,length(总长)=488+20=508B。封装第 2 片数据片的 IP 分组首部的 offset(片偏移)=488/8=61,length(总长)=488+20=508B。封装第 3 片数据片的 IP 分组首部的 offset(片偏移)=(2×488)/8=122,length(总长)=488+20=508B。封装第 4 片数据片的 IP 分组首部的 offset(片偏移)=(3×488)/8=183,length(总长)=16+20=36B。封装 4 片数据片的 IP 分组首部的 ID(标识)=6789,DF=0。封装前三个数据片的 IP 分组首部的 MF=1,封装最后一片数据片的 IP 分组首部的 MF=0。

9.2 选择题分析

(1) 以下哪一项不属于互连网安全技术?(　　)

A. 流量管制技术　　B. 防御路由项欺骗攻击技术

C. NAT　　D. 防御 MAC 表溢出攻击技术

答案: D

【分析】 互连网安全技术一般指网际层的安全技术。防御 MAC 表溢出攻击技术是以太网专用的安全技术。

(2) 以下哪一项有关安全路由的描述是错误的?(　　)

A. RIP 要求交换路由消息的两台相邻路由器配置相同的共享密钥

B. OSPF 要求属于同一区域的路由器接口配置相同的共享密钥

C. OSPF 要求建立邻接关系的两台相邻路由器配置相同的共享密钥

D. 路由消息必须携带共享密钥参与计算的消息鉴别码

答案: B

【分析】 路由消息鉴别发生在路由消息的发送路由器和路由消息的接收路由器之间。

(3) 以下哪一项是解决路由项欺骗攻击的机制?(　　)

A. 路由项源端鉴别和完整性检测机制

B. 路由项聚合机制

C. 手工配置静态路由项机制

D. 路由协议创建动态路由项机制

答案: A

【分析】 路由项欺骗的本质是没有授权发送路由消息的黑客终端发送了伪造的路由消息。因此,源端鉴别和完整性检测机制是保证接收到的路由消息是授权路由器发送,且传输过程中未被篡改的有效方法。采用手工配置所有路由项的方法,虽然也能解决路由项欺骗问题,但对于大型网络,手工配置所有路由项是很难做到的。

(4) 以下哪一项是实现路由项源端鉴别和完整性检测的前提?(　　)

A. 相邻路由器配置相同的共享密钥

B. 每一台路由器只能成为单台路由器的相邻路由器

C. 每一台路由器只允许启动一种路由协议

D. 只允许授权路由器向相邻路由器发送路由消息

答案：A

【分析】 相邻路由器之间配置相同的共享密钥，每一台路由器通过证明自己拥有共享密钥以证明自己是授权发送路由消息的路由器。

(5) 以下哪一项是隐藏内部网络的方法？(　　)

A. 其他路由器中手工配置用于指明通往内部网络的传输路径的静态路由项

B. 其他路由器中通过路由协议创建用于指明通往内部网络的传输路径的动态路由项

C. 其他路由器中没有用于指明通往内部网络的传输路径的路由项

D. 没有路由器接口连接内部网络

答案：C

【分析】 由于其他路由器中没有用于指明通往内部网络的传输路径的路由项，因此，内部网络对于这些路由器是透明的。

(6) 关于单播反向路径验证，以下哪一项描述是错误的？(　　)

A. 反向路径是指通往源终端的传输路径

B. 寻找反向路径时，用 IP 分组的源 IP 地址检索路由表

C. 用反向路径防御源 IP 地址欺骗攻击的前提是源和目的端之间的传输路径是对称的

D. 路由器路由表中分别创建用于指明正向路径和反向路径的路由项

答案：D

【分析】 路由器路由表中只有用于指明通往目的网络的传输路径的路由项。

(7) 关于策略路由，以下哪一项描述是错误的？(　　)

A. 针对特定目的终端，同时存在策略路由项和普通路由项

B. 策略路由项通过手工配置，普通路由项可以是直连路由项、静态路由项或动态路由项

C. 策略路由项的优先级高于普通路由项

D. 策略路由项是用于指明最短路径的路由项

答案：D

【分析】 策略路由项用于指明一条通往特定目的终端的传输路径，该传输路径不一定是距离最短的，有可能是传输延迟比较小的，或是经过路由器的安全性是有保障的等。

(8) 关于流量管制，以下哪一项描述是错误的？(　　)

A. 限制特定信息流的平均传输速率

B. 特定信息流可以用信息流的源和目的 IP 地址、协议类型等标识

C. 平均传输速率的上限是链路带宽

D. 平均传输速率是特定信息流的最大传输速率

答案：D

【分析】 平均传输速率是特定信息流时间周期 T 内的平均传输速率，允许特定信息流的实际传输速率短暂地超过平均传输速率。

(9) 关于令牌桶算法，以下哪一项描述是错误的？（　　）

A. 平均传输速率 $=R\times P/s$，其中 R 是令牌生成速率，P 是每一个令牌授权发送的二进制数位数

B. 允许持续以链路带宽发送的字节数 $=D\times P/8$，其中 D 是令牌桶深度，P 是每一个令牌授权发送的二进制数位数

C. 分组队列越大，最大传输延迟越高

D. 分组到达速率不能超过平均传输速率

答案：D

【分析】 由于存在分组队列，分组到达速率短暂地超过平均传输速率是允许的，但如果发生持续较长时间分组到达速率超过平均传输速率的情况，会导致分组队列溢出。

(10) 关于流量管制的作用，以下哪一项描述是错误的？（　　）

A. 能够有效防御 DoS　　B. 能够减轻病毒危害程度

C. 能够管控用户流量　　D. 能够阻止病毒传播

答案：D

【分析】 流量管制只能管控特定信息流的流量，不会检测信息流中是否携带病毒。因而无法阻止在允许流量内传播病毒的情况发生。

(11) 关于 NAT，以下哪一项描述是错误的？（　　）

A. 一种实现私有 IP 地址和全球 IP 地址相互转换的技术

B. 分配私有 IP 地址的内部网络对于公共网络是透明的

C. 建立私有 IP 地址和全球 IP 地址之间映射前，只能由内部网络终端发起访问外部网络的过程

D. 内部网络终端同时配置私有 IP 地址和全球 IP 地址

答案：D

【分析】 内部网络终端只配置私有 IP 地址，访问公共网络时，由互连内部网络和公共网络的边界路由器建立私有 IP 地址与全球 IP 地址之间的映射。

(12) NAT 对防止以下哪一项攻击是无效的？（　　）

A. 连接在公共网络上的黑客终端发起的对内部网络终端的主动攻击

B. 因为下载包含病毒的网页而感染病毒

C. 内部网络终端发起的对外部网络中的服务器的 SYN 泛洪攻击

D. 从外部网络传播蠕虫到内部网络

答案：B

【分析】 NAT 对内部网络终端访问外部网络或内部网络中的 Web 服务器没有限制。

(13) 关于无线路由器连接的内部网络和外部网络，以下哪一项描述是错误的？（　　）

A. 内部网络私有 IP 地址对外部网络是不可见的

B. 外部网络发送给内部网络的 IP 分组以无线路由器连接外部网络接口的 IP 地址为目的 IP 地址

C. 内部网络终端可以发起访问外部网络的过程

D. 外部网络终端可以发起访问内部网络的过程

答案：D

【分析】 内部网络终端发起访问外部网络的过程中，在无线路由器中建立地址转换项，通过地址转换项，建立内部网络终端的私有 IP 地址与特定标识信息之间的映射。在没有建立地址转换项之前，外部网络终端不能向内部网络终端发送 IP 分组。

(14) 关于 NAT，以下哪一项描述是错误的？(　　)

A. 内部网络发送给 Internet 的 IP 分组的净荷中携带唯一的标识信息

B. 无线路由器通过地址转换项建立私有 IP 地址与唯一的标识信息之间的映射

C. 外部网络回送给内部网络的 IP 分组的净荷中同样携带唯一的标识信息

D. 由内部网络终端生成发送给 Internet 的 IP 分组的净荷中的唯一标识信息

答案：D

【分析】 如果由各个内部网络终端独立生成发送给 Internet 的 IP 分组的净荷中的标识信息，不同终端有可能生成相同的标识信息，因此，这些标识信息是无法做到唯一的。要做到唯一，只能由无线路由器生成发送给 Internet 的 IP 分组的净荷中的标识信息。

(15) 如图 9.13 所示是 NAT 的一个示例，根据图 9.13 中的信息，编号为①的箭头线所对应的方框内容是(　　)。

A. S=192.168.1.1：3105
　D=202.113.64.2：8080

B. S=59.67.148.3：5234
　D=202.113.64.2：8080

C. S=192.168.1.1：3105
　D=59.67.148.3：5234

D. S=59.67.148.3：5234
　D=192.168.1.1：3105

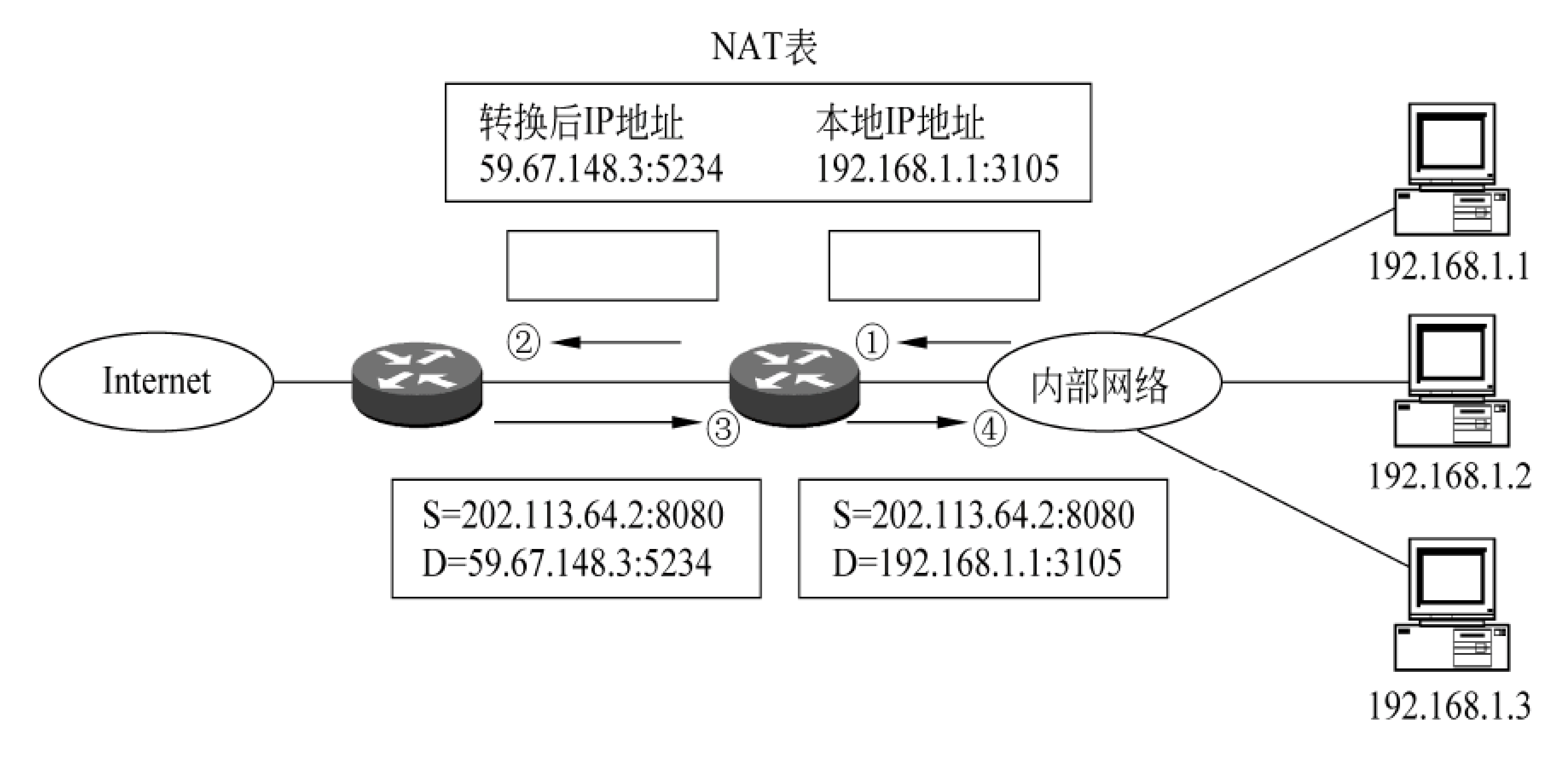


图 9.13　NAT 示例

答案：A

【分析】 编号为①的箭头线对应的方框中的源和目的地址信息与编号为④的箭头线对应的方框中的源和目的地址信息恰好相反。

(16) 如图 9.14 所示是 NAT 的一个示例,根据图 9.14 中的信息,标号为④的箭头线所对应的方框内容是(　　)。

A. S=135.2.1.1:80
D=202.0.1.1:5001

B. S=135.2.1.1:80
D=192.168.1.1:3342

C. S=135.2.1.1:5001
D=135.2.1.1:80

D. S=192.168.1.1:3342
D=135.2.1.1:80

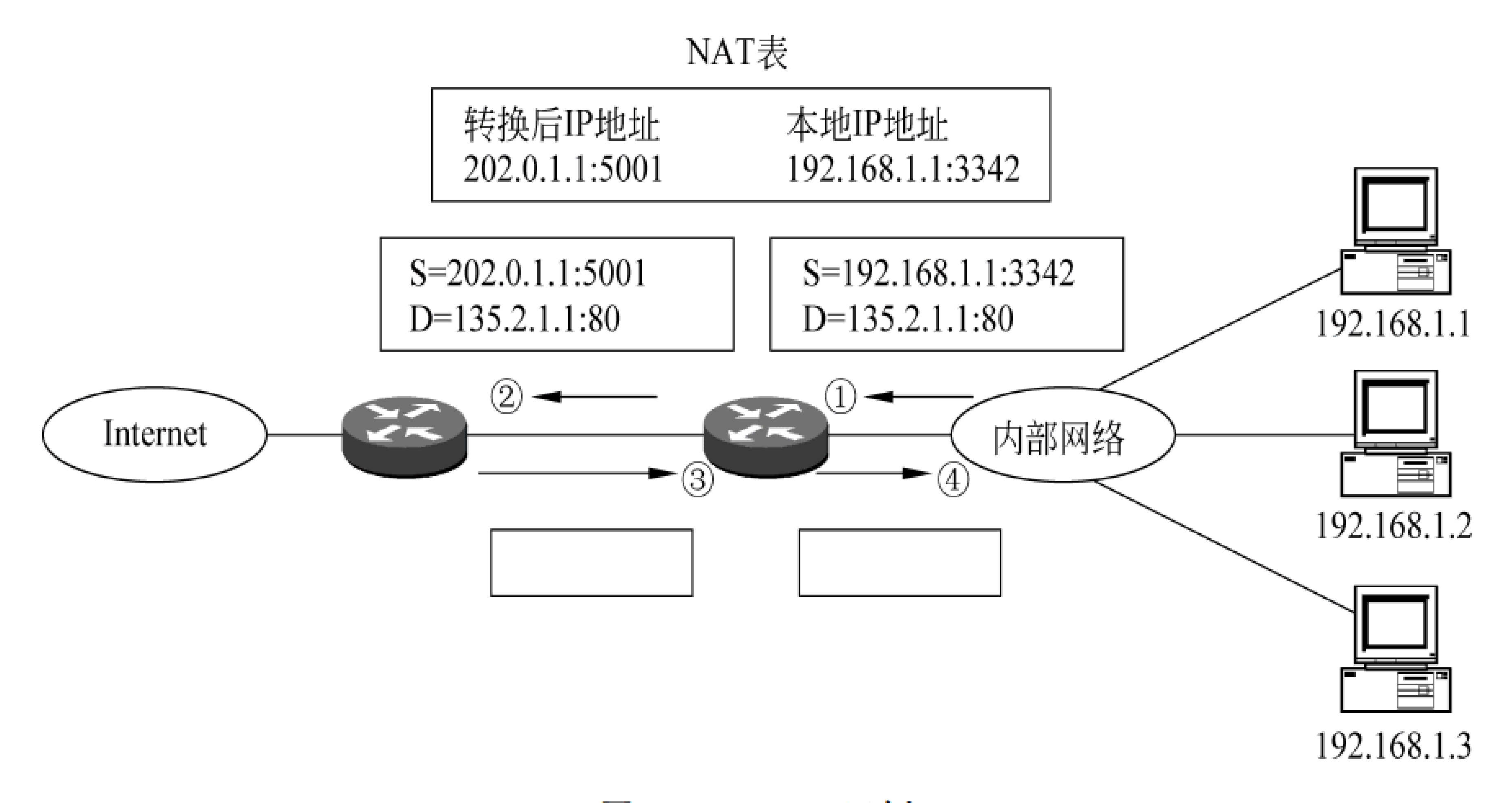


图 9.14　NAT 示例

答案:B

【分析】 编号为④的箭头线对应的方框中的源和目的地址信息与编号为①的箭头线对应的方框中的源和目的地址信息恰好相反。

(17) 如果需要将一个连接 10 台主机的内部网络接入 Internet,可以分配给内部网络的网络地址是(　　)。

A. 11.11.12.16/28　　B. 172.31.255.128/27

C. 192.168.1.0/28　　D. 209.165.202.128/28

答案:C

【分析】 只有 C 和 B 选项属于私有 IP 地址,但 B 选项可以有 30 个有效 IP 地址,C 选项只有 14 个有效 IP 地址,因此,C 选项更合适。

(18) 关于动态 PAT,以下哪一项描述是错误的?(　　)

A. 所有内部网络私有 IP 地址映射到唯一的全球 IP 地址

B. 动态建立全局唯一端口号或序号与私有 IP 地址之间映射

C. 全局唯一端口号或序号与私有 IP 地址之间映射以会话为单位

D. 会话只能是 TCP 连接

答案:D

【分析】 会话可以是一个 TCP 连接,也可以是 UDP 报文交换过程,也可以是一次 ICMP ECHO 请求和响应过程。

(19) 关于静态 PAT,以下哪一项描述是错误的?(　　)

A. 事先建立全局唯一端口号与私有 IP 地址之间映射

B. 实现公共网络终端发起访问内部网络的过程

C. 用多个不同的端口号映射多个不同的内部终端

D. 实现外部网络终端 ping 内部网络终端的过程

答案：D

【分析】 由于 ICMP ECHO 请求报文中的序号是本地唯一的，用于匹配 ICMP ECHO 响应报文，通常不能人工指定，因此，无法事先建立全局唯一序号与私有 IP 地址之间的映射。

(20) 关于动态 NAT，以下哪一项描述是错误的？(　　)

A. 同一时刻，不同的私有 IP 地址映射到不同的全球 IP 地址

B. 由内部网络终端发起建立全球 IP 地址与私有 IP 地址之间动态映射的过程

C. 全球 IP 地址与私有 IP 地址之间映射以会话为单位

D. 存在明显的创建会话和结束会话过程

答案：D

【分析】 许多情况下，以持续固定时间没有使用全球 IP 地址与私有 IP 地址之间动态映射实现地址转换的过程作为会话结束条件。

(21) 关于静态 NAT，以下哪一项描述是错误的？(　　)

A. 事先建立全球 IP 地址与私有 IP 地址之间的映射

B. 实现公共网络终端发起访问内部网络的过程

C. 用多个不同的全球 IP 地址映射多个不同的内部终端

D. 无法实现外部网络终端 ping 内部网络终端的过程

答案：D

【分析】 由于静态 NAT 固定建立某个私有 IP 地址与某个全球 IP 地址之间的映射，因此，外部终端可以用该全球 IP 地址访问配置该私有 IP 地址的终端，只要这种访问过程是基于 IP 的。

(22) 关于 VRRP，以下哪一项描述是错误的？(　　)

A. 一种有关冗余默认网关的协议

B. 可以由多台路由器组成一个虚拟路由器，虚拟路由器中存在主路由器和备份路由器

C. 虚拟路由器使用虚拟 IP 地址和虚拟 MAC 地址

D. 每一台路由器只能成为单个虚拟路由器的成员

答案：D

【分析】 每一台路由器可以成为多个虚拟路由器的成员，通常通过将某台路由器成为多个虚拟路由器成员，且在其中一个虚拟路由器中作为主路由器，在其他虚拟路由器中作为备份路由器以实现负载均衡。

(23) 关于 VRRP 生成主路由器过程，以下哪一项描述是错误的？(　　)

A. 如果存在多台主路由器，优先级最高的主路由器最终成为主路由器，其他成为备份路由器

B. 如果所有路由器都配置为不允许抢占方式，当主路由器失效后，并不一定是

优先级最高的备份路由器成为主路由器

C. 如果所有路由器都配置为允许抢占方式,优先级最高的路由器成为主路由器

D. 如果所有路由器都配置为不允许抢占方式,则路由器的优先级是无用的

答案:D

【分析】 即使所有路由器都配置为不允许抢占方式,当虚拟路由器中存在多台主路由器时,需要通过优先级决定最终唯一的主路由器。

9.3 名词解释

(1) 安全路由

一种保证路由表中路由项正确,且能够对传输的 IP 分组的源 IP 地址进行检测的安全技术。

(2) 流量管制

一种限制路由器接口输入/输出特定信息流的流量的安全技术。

(3) NAT

一种既能隐藏分配私有 IP 地址的内部网络,又能使分配私有 IP 地址的内部网络终端能够发起访问公共网络的过程的安全技术。

(4) VRRP

一种通过默认网关冗余,使终端在默认网关失效的情况下,无须修改默认网关地址,便可继续与其他网络中的终端交换 IP 分组的协议。

(5) 防路由项欺骗攻击机制

一种通过对路由消息进行源端鉴别和完整性检测,保证路由表中的路由项正确有效的机制。

(6) 路由项过滤

一种通过限制某个接口发送的路由消息中包含的路由项,使该路由器可以到达的某些网络对于其他路由器是透明的安全技术。

(7) 单播反向路径验证

一种基于对称的端到端传输路径检测 IP 分组中源 IP 地址是否是伪造的 IP 地址的安全技术。

(8) 策略路由

一种用于为符合特定条件的 IP 分组选择特殊的传输路径的路由技术。

(9) PAT

一种用于建立全局唯一端口号,或者全局唯一序号与内部网络私有 IP 地址之间映射的 NAT 技术。

第10章 虚拟专用网络

10.1 例题解析

10.1.1 简答题解析

【例题10.1】 简述隧道和IPSec是实现VPN的基础的理由。

【解析】 隧道是一种通过公共网络传输任意格式分组的技术,任意格式分组封装后可以作为以隧道两端IP地址为源和目的IP地址的外层IP分组的净荷,在完成外层IP分组隧道两端之间传输的同时,实现任意格式分组隧道一端至隧道另一端的传输过程。

IPSec能够实现IP分组净荷隧道两端之间的安全传输过程。隧道与IPSec结合可以实现任意格式分组公共网络任意两个端点之间的安全传输过程。这恰恰是VPN的设计目标,用公共网络实现内部网络各个子网之间的互连,同时又能保证内部网络封装形式的数据各个子网间的安全传输。

【例题10.2】 简述VPN和NAT的区别和联系。

【解析】 VPN的设计目标是用公共网络实现内部网络各个子网之间的互连,同时又能保证内部网络封装形式的数据在各个子网间的安全传输。因此,VPN主要用于实现通过公共网络互连的内部网络在各个子网间的安全通信。NAT主要用于实现内部网络终端与公共网络终端之间的通信过程。在只需要实现内部网络终端之间通信过程的VPN中,公共网络对于内部网络终端是透明的。VPN不需要NAT技术,但如果某个VPN既要实现内部网络终端之间的通信过程,又要实现内部网络终端与公共网络终端之间的通信过程,则需要在隧道和IPSec的技术上增加NAT技术。

【例题10.3】 简述Cisco Easy VPN与点对点隧道和IPSec的区别。

【解析】 一是点对点隧道两端需要配置匹配的ISAKMP策略和IPSec变换集,但Cisco Easy VPN往往只需在VPN服务器上配置ISAKMP策略和IPSec变换集,在建立IPSec安全关联过程中由VPN服务器将ISAKMP策略和IPSec变换集推送给远程终端。二是Cisco Easy VPN需要以组为单位组织远程终端,属于同一组的远程终端使用相同的共享密钥和内部网络配置信息,但可以具有不同的身份标识信息。三是Cisco Easy VPN需要创建动态加密映射,允许任何IPSec安全关联发起者成为该动态加密映射的另一端。四是VPN服务器在成功建立安全传输通道后,需要鉴别远程终端身份,并在成功鉴别远程终端身份后,向远程终端推送内部网络配置信息,如内部网络私有IP地址和子网掩码等。五是点对点隧道在创建隧道时,通过在隧道两端静态配置内部网络私有IP地址和路

由协议,动态建立用于指明通往内部网络各个子网的传输路径的路由项。但 Cisco Easy VPN 不需要静态配置 VPN 服务器与远程终端之间的隧道,在成功建立与某个远程终端之间的 IPSec 安全关联后,动态创建 VPN 服务器与远程终端之间的隧道,并建立用于指明内部网络内通往该远程终端的传输路径的路由项。

10.1.2 设计题解析

【例题 10.4】 第三层隧道+IPSec VPN 如图 10.1 所示,给出能够实现终端 A 和终端 C 之间相互通信的路由器 R1、R2 的配置(包括路由表和隧道)和隧道报文封装过程。

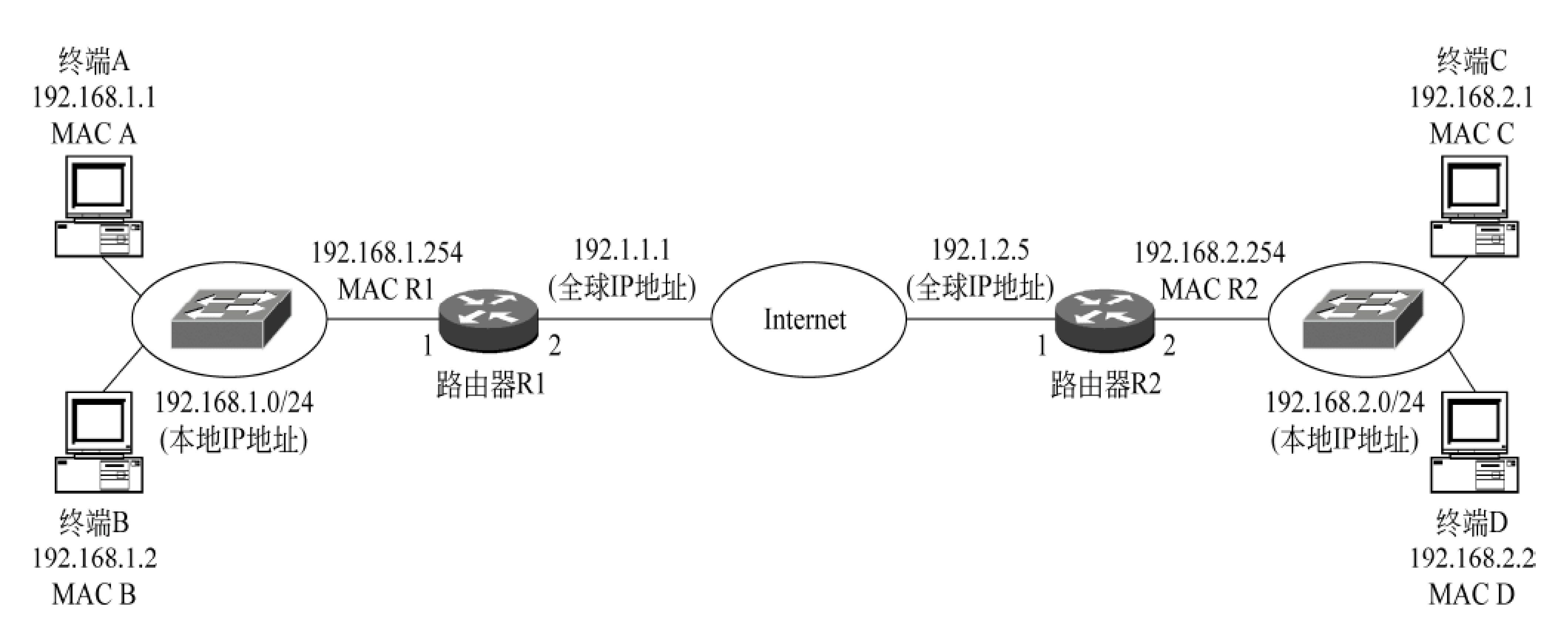


图 10.1 第三层隧道+IPSec VPN 结构

【解析】

对于边界路由器 R1,隧道源端全球 IP 地址是 192.1.1.1,隧道目的端全球 IP 地址是 192.1.2.5。

对于边界路由器 R2,隧道源端全球 IP 地址是 192.1.2.5,隧道目的端全球 IP 地址是 192.1.1.1。

需要为隧道两端分配私有 IP 地址,隧道路由器 R1 一端的私有 IP 地址是 192.168.3.1,隧道路由器 R2 一端的私有 IP 地址是 192.168.3.2。

路由器 R1 路由表如表 10.1 所示,由两类路由项组成,一类是用于指明通往内部网络各个子网的传输路径的路由项,其中通往子网 192.168.2.0/24 的传输路径的下一跳是隧道路由器 R2 一端的私有 IP 地址 192.168.3.2。另一类是用于指明 Internet 中通往隧道另一端的传输路径的路由项,其中通往全球 IP 地址为 192.1.2.5 的隧道目的端的传输路径的下一跳是 Internet 中直接与路由器 R1 相连的某台路由器,表 10.1 中用 Internet 中的下一跳表示。路由器 R2 路由表如表 10.2 所示。

表 10.1 边界路由器 R1 路由表

目的网络地址	子网掩码	输出接口	下一跳路由器
192.168.1.0	255.255.255.0	1	直接
192.168.2.0	255.255.255.0	隧道	192.168.3.2
192.1.2.5	255.255.255.255	2	Internet 中的下一跳

表 10.2　边界路由器 R2 路由表

目的网络地址	子 网 掩 码	输 出 接 口	下一跳路由器
192.168.1.0	255.255.255.0	隧道	192.168.3.1
192.168.2.0	255.255.255.0	2	直接
192.1.1.1	255.255.255.255	1	Internet 中的下一跳

终端 A 发送给终端 C 的 IP 分组，经过隧道传输时的封装过程如图 10.2 所示，首先将以终端 A 的私有 IP 地址为源 IP 地址、以终端 C 的私有 IP 地址为目的 IP 地址的内层 IP 分组封装成 GRE 格式，然后将 GRE 格式作为净荷，封装成以边界路由器 R1 连接 Internet 的接口的全球 IP 地址为源 IP 地址、以边界路由器 R2 连接 Internet 的接口的全球 IP 地址为目的 IP 地址的外层 IP 分组。

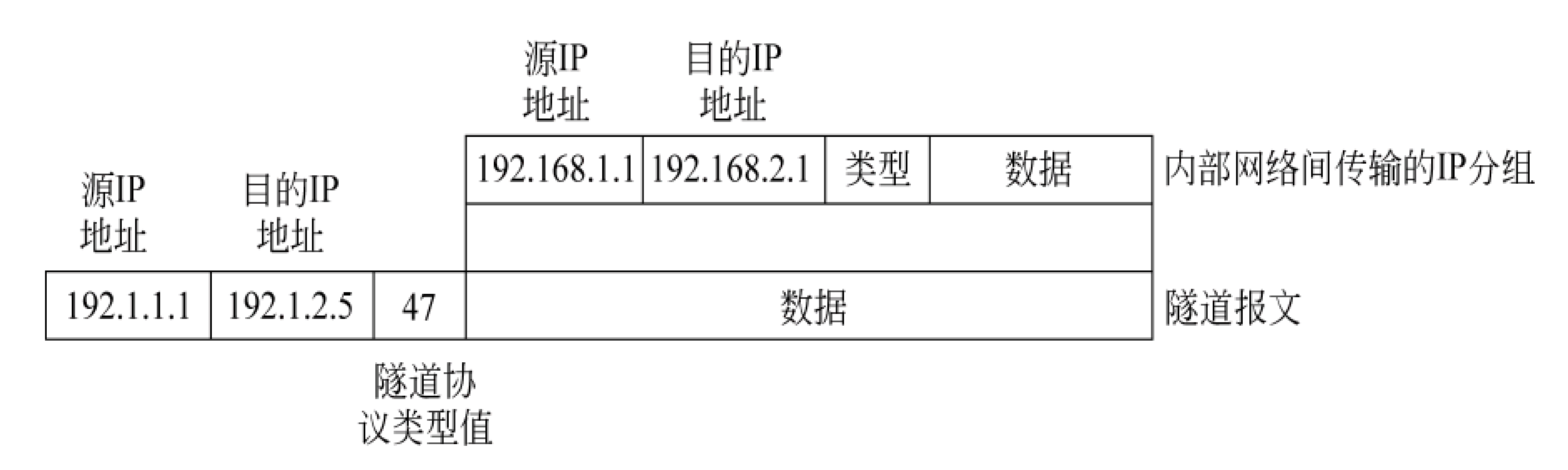


图 10.2　隧道报文封装过程

【例题 10.5】 第三层隧道+IPSec VPN 如图 10.1 所示，给出能够实现终端 A 和终端 C 之间安全通信的路由器 R1、R2 的配置(包括安全关联相关参数、IP 分组分类标准等)和 ESP 报文封装过程。

【解析】

(1) 路由器 R1 和 R2 IKE 安全关联相关参数如下。

身份鉴别机制：证书+私钥。

加密算法：3DES。

报文摘要算法：MD5。

密钥分发协议：Diffie-Hellman，选择组号为 2 的参数。

(2) 路由器 R1 和 R2 IPSec 安全关联相关参数如下。

安全协议：ESP。

加密算法：AES。

MAC 算法：HMAC-MD5-96。

(3) 路由器 R1 分类标准如下。

源 IP 地址：192.1.1.1。

目的 IP 地址：192.1.2.5。

协议：GRE。

(4) 路由器 R2 分类标准如下。

源 IP 地址：192.1.2.5。

目的 IP 地址：192.1.1.1。

协议类型：GRE。

(5) 终端 A 发送给终端 C 的 IP 分组，经过隧道传输时封装成 ESP 报文的过程如图 10.3 所示。首先将终端 A 发送给终端 C 的内层 IP 分组封装成以边界路由器 R1 连接 Internet 的接口的全球 IP 地址为源 IP 地址、以边界路由器 R2 连接 Internet 的接口的全球 IP 地址为目的 IP 地址的外层 IP 分组，然后将外层 IP 分组封装成 ESP 报文。

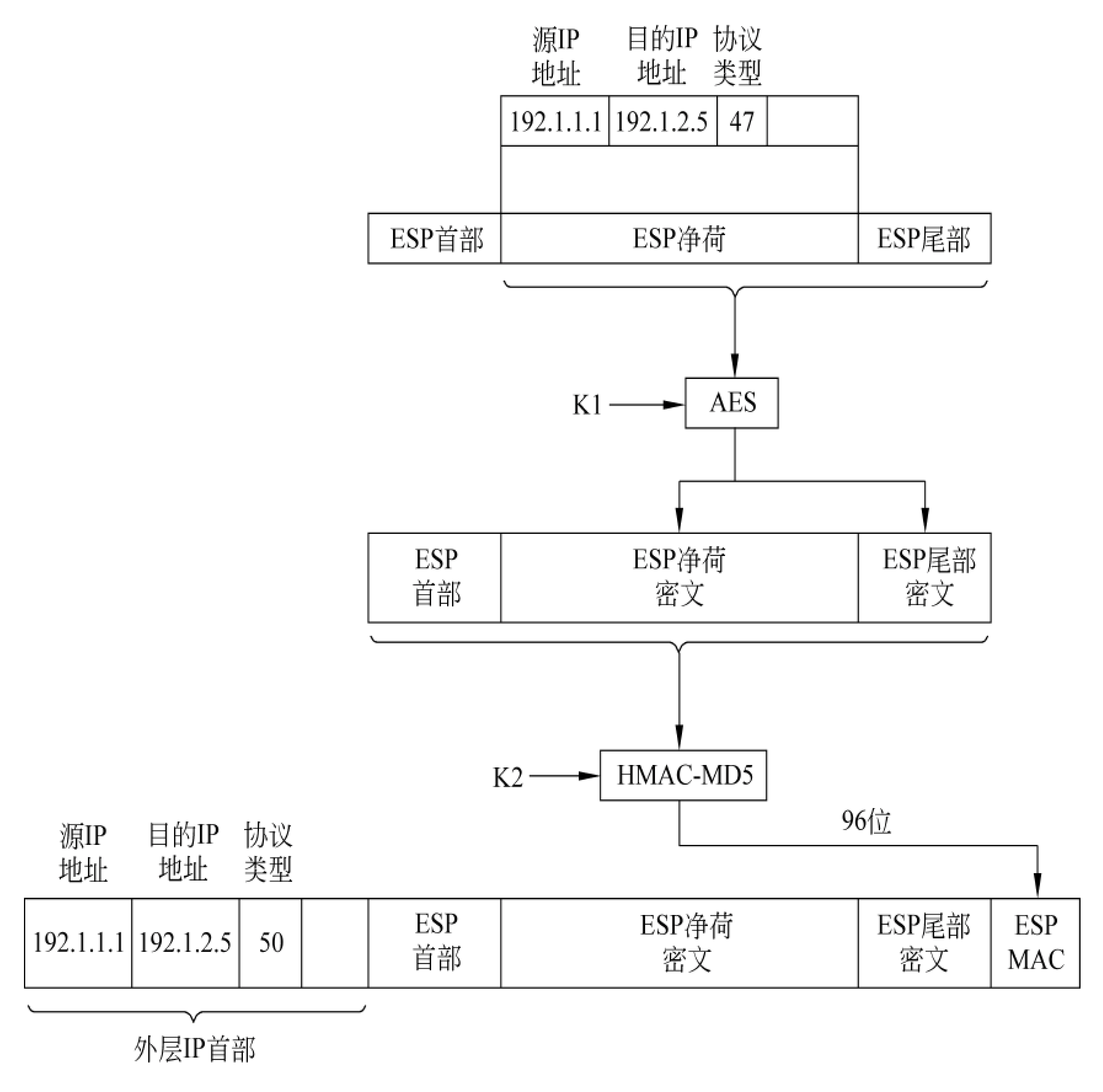


图 10.3　ESP 报文封装过程

【例题 10.6】 网络结构如图 10.4 所示，企业内部网络分配本地 IP 地址，远程接入用户如何通过 VPN 像企业内部网络中的本地终端一样访问企业内部网络资源，给出实

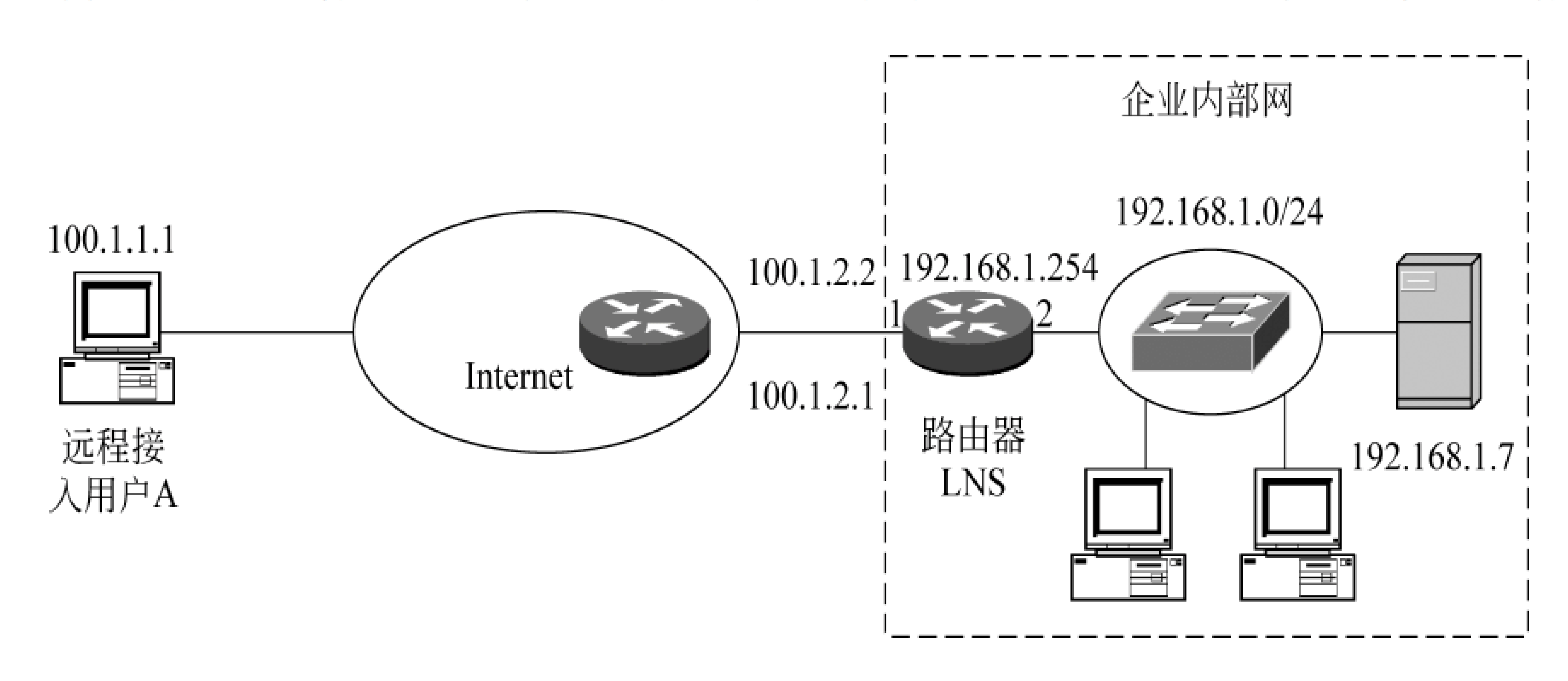


图 10.4　远程接入过程

现这一功能所要求的配置信息和远程接入用户访问企业内部网络资源的过程。

【解析】

(1) 远程终端配置信息

第二层隧道控制协议：L2TP。

LNS 地址：100.1.2.1。

用户名：用户 A。

密码：PASSA。

鉴别协议：CHAP。

(2) LNS 配置信息

第二层隧道控制协议：L2TP。

本地 IP 地址池：192.168.2.1～192.168.2.100。

注册用户库如表 10.3 所示。

表 10.3　注册用户库

用　户　名	密　　码	鉴 别 协 议
用户 A	PASSA	CHAP

(3) 远程接入用户访问企业内部网络资源的过程

① 通过 L2TP 建立远程终端与 LNS 之间的第二层隧道。

② 远程终端与 LNS 之间建立基于第二层隧道的 PPP 链路。

③ LNS 完成对远程终端用户的身份鉴别过程。

④ LNS 在本地 IP 地址池中选择一个未使用的本地 IP 地址(如 192.168.2.1),将其分配给远程终端,并在路由表中创建一项将该本地 IP 地址和远程终端与 LNS 之间的第二层隧道绑定在一起的路由项。

⑤ 远程终端用 LNS 分配的本地 IP 地址,像企业内部网络中的终端一样访问企业内部网络资源。

【例题 10.7】 网络结构如图 10.5 所示,要求对终端访问服务器(Web 服务器和 FTP 服务器)过程实施统一控制,访问对象能够精确到文件,在网络中增加必要的设备,并给出与实施统一访问控制有关的配置信息。

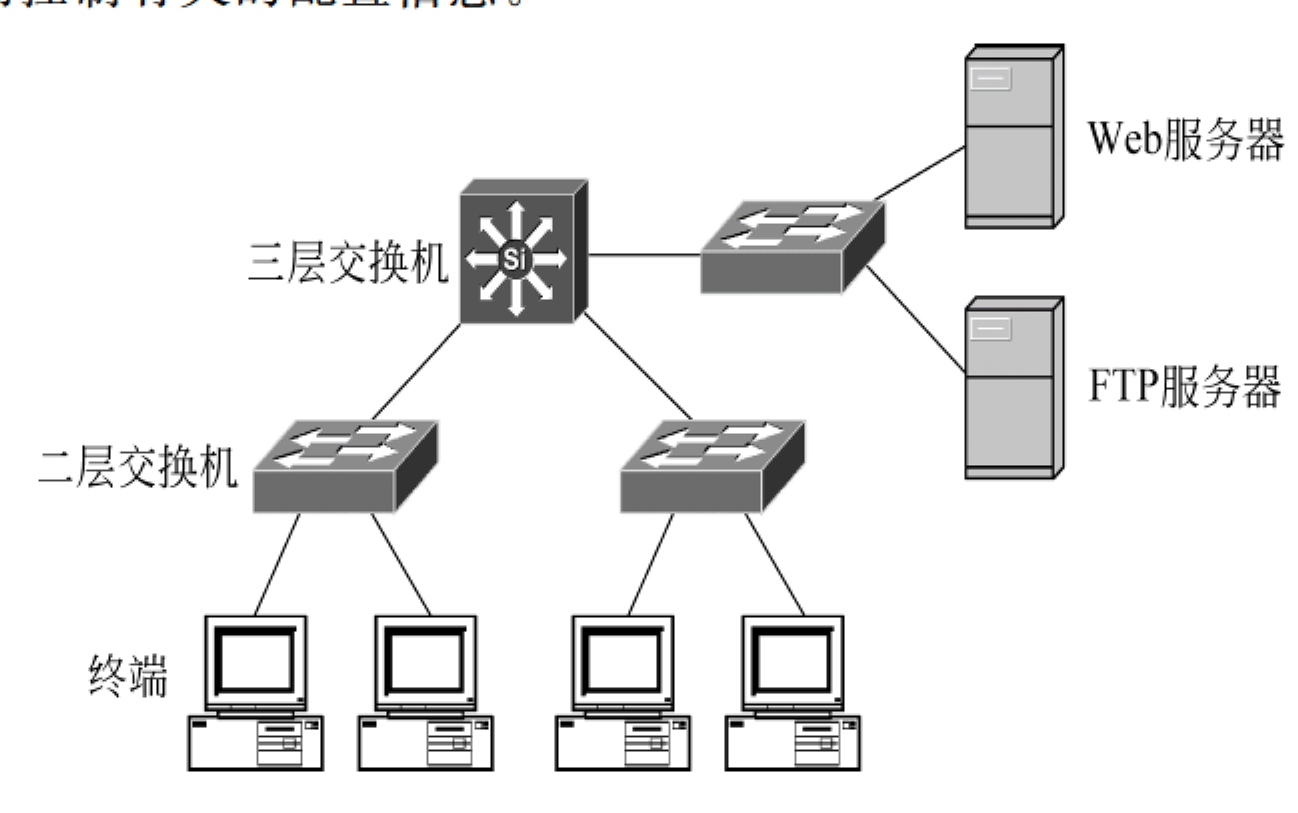


图 10.5　网络结构

【解析】

(1) 增加 SSL VPN 网关,SSL VPN 网关位置如图 10.6 所示。

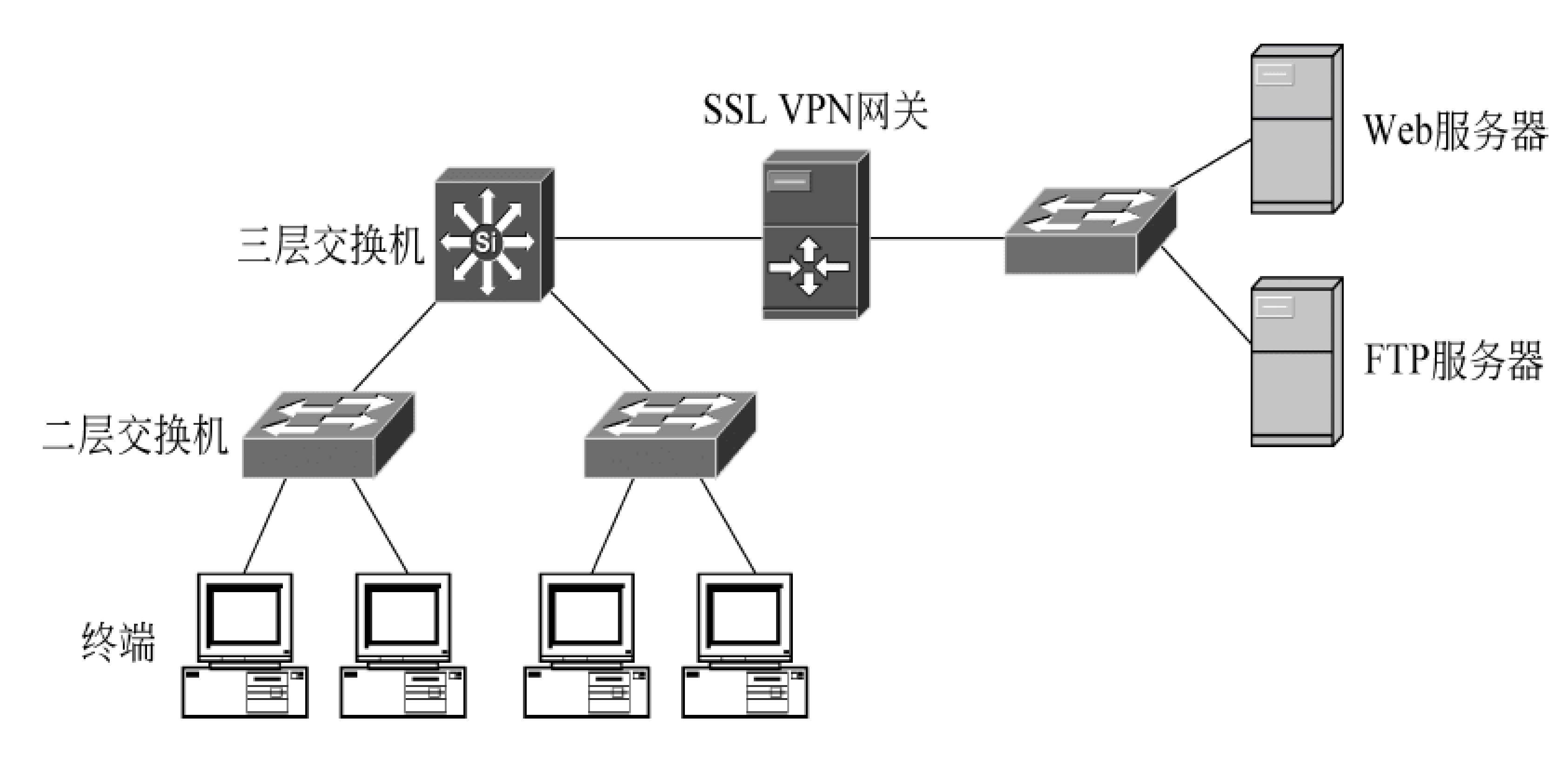


图 10.6 SSL VPN 结构

(2) SSL VPN 网关完成证书申请过程,其他终端能够获取证明 SSL VPN 网关完全合格的域名与其公钥之间绑定关系的证书。

(3) SSL VPN 网关配置如表 10.4 所示的注册用户库,注册用户库中列出所有注册用户的用户名和密码。

(4) 为每一个注册用户分配访问权限,建立如表 10.5 所示的用户权限表。用户权限用该注册用户能够访问的对象表示,每一个对象用 URL 唯一标识。

(5) 每一个注册用户可以登录 SSL VPN 网关,成功登录后,给出 URL 列表,URL 列表中是一组标识授权该注册用户访问的对象的 URL。

表 10.4 注册用户库

用户名	密码
用户 A	PASSA
用户 B	PASSB

表 10.5 用户权限表

用户名	访问权限
用户 A	URL1
用户 A	URL2
用户 B	URL3

10.2 选择题分析

(1) 关于 VPN,以下哪一项描述是错误的?( )

A. 实现由公共网络分隔的、分配私有 IP 地址的内部网络各个子网之间的通信过程

B. 保障内部网络各个子网之间传输的信息的保密性

C. 保障内部网络各个子网之间传输的信息的完整性

D. 互连内部网络各个子网的只能是专用点对点物理链路

答案:D

【分析】 实现内部网络各个子网之间互连的可以是 Internet,而且可以采用任何接

入技术将内部网络各个子网接入到 Internet。

(2) 关于 VPN,以下哪一项描述是正确的?(　　)

A. 内部网络各个子网分配的网络地址不能相同

B. 内部网络各个子网分配的网络地址可以相同

C. 某个内部网络子网对其他内部网络子网是透明的

D. 某个内部网络子网分配的私有 IP 地址对其他内部网络子网是透明的

答案:A

【分析】 内部网络是由各个子网互连而成的互连网,因此,每一个子网必须分配不同的网络地址。

(3) 下列技术中,哪一项不能有效防范网络嗅探攻击?(　　)

A. VPN　　B. SSL　　C. Telnet　　D. SSH

答案:C

【分析】 由于 Telnet 以明文方式传输登录时使用的用户名和密码,因此黑客很容易通过嗅探攻击获取某个注册用户登录时使用的用户名和密码。

(4) 关于专用网络,以下哪一项描述是错误的?(　　)

A. 专用网络各个子网可以分配私有 IP 地址

B. 企业拥有专用网络全部资源

C. 专用网络内传输的信息是相对安全的

D. 专用网络便于扩展

答案:D

【分析】 由于路由器之间通过专用物理链路实现互连,因此,增加或删除专用网络中的子网是一件麻烦的事情。

(5) 以下哪一项不是专用网络的缺陷?(　　)

A. 运行成本高　　B. 不便于扩展

C. 实现难度大　　D. 安全性差

答案:D

【分析】 由于企业拥有专用网络的全部资源,因此,专用网络内传输的信息不容易被外部人员嗅探和截获,是相对安全的。

(6) 以下哪一项不是专用网络的特点?(　　)

A. 使用私有 IP 地址　　B. 不和其他网络共享传输路径

C. 不能和其他网络相互通信　　D. 使用 TCP/IP 协议栈

答案:D

【分析】 并不只有专用网络使用 TCP/IP 协议栈。

(7) 以下哪一项是虚拟专用网络有别于专用网络的地方?(　　)

A. 使用私有 IP 地址

B. 实现数据内部网络子网间的安全传输

C. 使用公共网络提供的数据传输通路

D. 使用 TCP/IP 协议栈

答案：C

【分析】 虚拟专用网络用隧道实现内部网络各个子网间的互连，隧道两端之间的传输路径经过公共网络，且内部网络不能独占隧道两端之间传输路径经过的物理链路的带宽。

(8) 以下哪一项不是虚拟专用网络需要解决的问题？(　　)

A. 使用私有 IP 地址的 IP 分组如何经过 Internet 传输的问题

B. 如何保证经过 Internet 传输的数据的安全的问题

C. 如何防止其他网络冒充内部网络子网的问题

D. 如何实现内部网络终端和公共网络终端之间通信的问题

答案：D

【分析】 VPN 的主要任务不是实现内部网络终端与公共网络终端之间的通信过程。

(9) 对于远程接入过程，以下哪一项描述是错误的？(　　)

A. 通过 PSTN 建立远程终端与接入控制设备之间的语音信道

B. 远程终端与接入控制设备之间带宽受限

C. 接入费用较高

D. 安全性差

答案：D

【分析】 由于远程终端与接入控制设备之间通过语音信道互连，而经过语音信道传输的信息是相对安全的。

(10) 以下哪一项不是 VPN 需要解决的问题？(　　)

A. 实现由互连网分隔的两个分配私有 IP 地址的终端之间相互通信的问题

B. 保证经过互连网传输的数据的保密性和完整性的问题

C. 由互连网互连的内部网络边界路由器之间的双向身份鉴别问题

D. 在互连网中建立内部网络边界路由器之间的传输路径的问题

答案：D

【分析】 建立连接在互连网中任意两个节点之间的传输路径是互连网的基本功能，不是 VPN 特有的。

(11) 关于隧道，以下哪一项描述是错误的？(　　)

A. 一种实现互连网两端之间无法直接经过互连网传输的 PDU 的传输过程的技术

B. 隧道报文通常是以隧道两端全球 IP 地址为源和目的 IP 地址的 IP 分组

C. 无法直接经过互连网传输的 PDU 作为隧道报文的净荷

D. 直接转换无法直接经过互连网传输的 PDU 中的私有 IP 地址

答案：D

【分析】 无法直接经过互连网传输的 PDU 作为以隧道两端全球 IP 地址为源和目的 IP 地址的隧道报文的净荷，经过互连网传输的是隧道报文。

(12) 关于隧道，以下哪一项描述是错误的？(　　)

A. 隧道两端分配全球 IP 地址

B. 隧道两端可以实现双向身份鉴别

C. 保障经过隧道传输的数据的保密性和完整性

D. 隧道是互连网中隧道两端专用的传输路径

答案：D

【分析】 隧道只是互连网中实现以隧道两端全球 IP 地址为源和目的 IP 地址的隧道报文隧道两端之间传输过程的传输路径。互连网中其他节点之间的传输过程可以共享隧道经过的传输路径。

(13) 以下哪一项不是目前常见的 VPN 类型？(　　)

A. IPSec 第三层隧道　　B. IPSec 第二层隧道

C. SSL VPN　　D. PPPoE VPN

答案：D

【分析】 VPN 需要满足以下两点要素：一是实现互连网两端之间无法直接经过互连网传输的 PDU 的传输过程；二是保障经过互连网传输的数据的保密性和完整性。

(14) 关于隧道，以下哪一项描述是错误的？(　　)

A. 隧道两端是分配全球 IP 地址的两个接口

B. 允许多种不同封装格式的分组从隧道一端传输到隧道另一端

C. 经过隧道传输的分组对隧道两端之间的 IP 传输路径是透明的

D. 经过隧道传输的必须是传输层以上的 PDU

答案：D

【分析】 链路层帧可以作为第二层隧道的净荷，因此，IPSec 和隧道结合可以经过 IP 传输路径安全传输链路层帧。

(15) 关于第三层隧道，以下哪一项描述是正确的？(　　)

A. 隧道报文中的净荷是以私有 IP 地址为源和目的 IP 地址的 IP 分组

B. 隧道报文中的净荷是 PPP 帧

C. 隧道报文中的净荷是 HTTP 消息

D. 隧道报文中的净荷是以全球 IP 地址为源和目的 IP 地址的 IP 分组

答案：A

【分析】 经过第三层隧道传输的且无法直接经过互连网传输的 PDU 是以私有 IP 地址为源和目的 IP 地址的 IP 分组。

(16) 关于第二层隧道，以下哪一项描述是正确的？(　　)

A. 隧道报文中的净荷是以私有 IP 地址为源和目的 IP 地址的 IP 分组

B. 隧道报文中的净荷是 PPP 帧

C. 隧道报文中的净荷是 HTTP 消息

D. 隧道报文中的净荷是以全球 IP 地址为源和目的 IP 地址的 IP 分组

答案：B

【分析】 PPP 帧是其中一种经过第二层隧道传输的且无法直接经过互连网传输的 PDU。

(17) 对于 IPSec 第三层隧道 VPN，互连内部网络与 Internet 的边界路由器的路由表

中不包含以下哪类路由项？（　　）

A. 用于指明通往内部网络各个子网的传输路径的路由项

B. 用于指明通往隧道另一端的传输路径的路由项

C. 用于指明通往直接连接的内部网络子网和互连网子网的传输路径的路由项

D. 用于指明通往互连网中所有子网的传输路径的路由项

答案：D

【分析】 作为边界路由器，与互连网相关的路由项通常只需要包含用于指明通往隧道另一端的传输路径的路由项。

（18）对于 IPSec 第三层隧道 VPN，以下哪一项不是 IPSec 实现的功能？（　　）

A. 隧道两端之间双向身份鉴别

B. 隧道两端之间传输的数据的保密性

C. 隧道两端之间传输的数据的完整性

D. 以私有 IP 地址为源和目的 IP 地址的 IP 分组跨互连网传输过程

答案：D

【分析】 这是隧道实现的功能。

（19）以下哪一项不是 IPSec 提供的功能？（　　）

A. 实现使用私有 IP 地址的 IP 分组经过 Internet 传输

B. 保证经过 Internet 传输的数据的安全性

C. 实现数据的源端鉴别

D. 实现源端和目的端之间的相互身份鉴别

答案：A

【分析】 该项功能由隧道实现，VPN 的技术基础是隧道和 IPSec。

（20）关于传统拨号接入过程，以下哪一项描述是错误的？（　　）

A. 拨号建立远程终端与接入控制设备之间的点对点语音信道

B. 基于语音信道建立 PPP 链路

C. 接入控制设备基于 PPP 链路完成对远程终端的身份鉴别过程

D. 远程终端与内部网络交换的数据直接封装成 PPP 帧

答案：D

【分析】 远程终端与内部网络交换的数据先封装成 IP 分组，然后将 IP 分组封装成 PPP 帧。

（21）关于 IPSec 第二层隧道 VPN，以下哪一项描述是错误的？（　　）

A. 建立基于第二层隧道的 PPP 链路

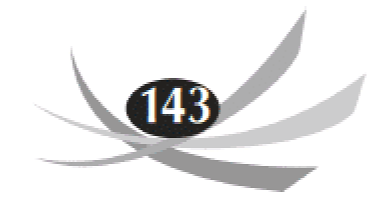
B. 接入控制设备基于 PPP 链路完成对远程终端的身份鉴别过程

C. 接入控制设备对远程终端分配内部网络私有 IP 地址

D. 直接经过第二层隧道传输构成 PPP 帧的字节流

答案：D

【分析】 第二层隧道是虚拟点对点链路，不能直接传输构成 PPP 帧的字节流。需要将 PPP 帧封装成以第二层隧道两端的全球 IP 地址为源和目的 IP 地址的隧道报文，第二



层隧道传输的是隧道报文。

(22) 关于 IPSec 第二层隧道 VPN 的封装过程，以下哪一项描述是错误的？(　　)

A. 以私有 IP 地址为源和目的 IP 地址的 IP 分组封装成 PPP 帧

B. PPP 帧封装成第二层隧道格式

C. 第二层隧道格式封装成以隧道两端全球 IP 地址为源和目的 IP 地址的隧道报文

D. 第二层隧道用隧道两端的全球 IP 地址唯一标识

答案：D

【分析】 每一个远程终端与接入控制设备之间有着独立的第二层隧道，用不同的会话标识符标识各个独立的第二层隧道。

(23) 关于第二层隧道建立过程，以下哪一项描述是正确的？(　　)

A. 建立远程终端与接入控制设备之间的点对点物理链路

B. 建立远程终端与接入控制设备之间的 IP 传输路径

C. 基于点对点物理链路建立 PPP 链路

D. 完成会话标识符分配和链路类型协商过程

答案：D

【分析】 由互连网完成建立远程终端与接入控制设备之间的 IP 传输路径的过程，第二层隧道的建立过程其实就是隧道两端完成会话标识符分配和链路类型协商的过程。

(24) 关于 L2TP 控制连接建立过程，以下哪一项描述是错误的？(　　)

A. 完成 LAC 与 LNS 之间的双向身份鉴别

B. LAC 和 LNS 分配本地控制连接标识符

C. 双方约定支持的虚拟线路类型

D. 建立 LAC 与 LNS 之间的点对点物理链路

答案：D

【分析】 所谓的控制连接建立过程，其实就是 LAC 与 LNS 之间为安全、可靠传输 L2TP 控制消息而完成的一次协商过程，并不存在建立 LAC 与 LNS 之间的点对点物理链路的过程。

(25) 关于第二层隧道建立过程，以下哪一项描述是错误的？(　　)

A. LAC 和 LNS 分配本地会话标识符

B. LAC 和 LNS 约定虚拟线路类型

C. 确定经过第二层隧道传输的链路层帧类型

D. 建立第二层隧道经过的 IP 传输路径

答案：D

【分析】 所谓的第二层隧道建立过程，只是一个在第二层隧道两端之间协商第二层隧道的类型，分配会话标识符和 Cookie 的过程，不存在建立实际的第二层隧道两端之间 IP 传输路径的过程。

(26) 关于第二层隧道，以下哪一项描述是错误的？(　　)

A. 第二层隧道是基于 LAC 和 LNS 之间 IP 传输路径的虚拟物理链路

B. 可以建立基于第二层隧道的 PPP 链路

C. 可以经过 PPP 链路传输 PPP 帧

D. 可以经过 LAC 与 LNS 之间的第二层隧道直接传输 PPP 帧

答案：D

【分析】 由于第二层隧道是基于 LAC 和 LNS 之间 IP 传输路径的虚拟物理链路，因此，PPP 帧只有封装成以 LAC 和 LNS 的全球 IP 地址为源和目的 IP 地址的 IP 分组后，才能经过 LAC 和 LNS 之间的 IP 传输路径传输。

(27) 关于 IP Sec 第二层隧道 VPN 的缺陷，以下哪一项描述是错误的？(　　)

A. 终端需要配置与建立 IKE 安全关联相关的参数

B. 终端需要配置与建立 IPSec 安全关联相关的参数

C. 终端配置的安全参数必须与 LNS 配置的安全参数一致

D. 终端发起远程接入过程

答案：D

【分析】 无论何种远程终端接入内部网络的过程，通常都是由远程终端发起接入内部网络的过程。

(28) 以下哪一项和 VPN 接入无关？(　　)

A. 远程终端分配内部网络私有 IP 地址

B. 连接 Internet 的远程终端访问内部网络中的资源

C. 建立远程终端与内部网络连接 Internet 的路由器之间的安全隧道

D. 远程终端拨号接入方式接入 Internet

答案：D

【分析】 远程终端需要连接在 Internet 上，分配全球 IP 地址，但无须指定远程终端接入 Internet 的方式。

(29) 关于 SSL VPN，以下哪一项描述是错误的？(　　)

A. 终端客户端可以是浏览器

B. 可以基于用户分配访问权限

C. 用于实现连接在互连网上的远程终端访问内部网络资源的过程

D. 需要建立基于远程终端与 SSL VPN 网关之间 IP 传输路径的第三层隧道

答案：D

【分析】 连接在互连网上的远程终端分配全球 IP 地址，直接访问同样连接在互连网上、分配全球 IP 地址的 SSL VPN 网关。远程终端与 SSL VPN 网关之间直接传输以远程终端和 SSL VPN 网关的全球 IP 地址为源和目的 IP 地址的 IP 分组。

(30) 关于家庭局域网中分配私有 IP 地址的终端，以下哪一项描述是正确的？(　　)

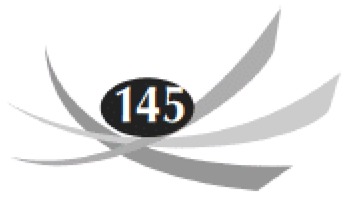
A. 通过 SSL VPN 远程接入内部网络

B. 通过 IPSec 第二层隧道 VPN 远程接入内部网络

C. 通过 IPSec 第三层隧道 VPN 远程接入内部网络

D. 通过 Cisco Easy VPN 远程接入内部网络

答案：A



【分析】 家庭局域网中分配私有 IP 地址的终端只能通过 SSL VPN 远程接入内部网络。

10.3　名词解释

(1) VPN

一种通过 Internet 实现企业局域网之间互连和远程终端与内部网络之间互连，但又使其具有专用网络所具有的安全性的技术。

(2) 企业专用网络

由专用的点对点物理链路实现各个子网之间互连的企业网。

(3) 远程接入过程

一个与内部网络相隔甚远的终端接入内部网络，并访问内部网络资源的过程。

(4) 隧道

一种实现互连网两端之间无法直接经过互连网传输的 PDU 的传输过程的技术。

(5) IPSec 第三层隧道 VPN

一种通过隧道实现以私有 IP 地址为源和目的 IP 地址的 IP 分组跨互连网传输的过程，通过 IPSec 实现经过隧道传输的数据的保密性和完整性的 VPN。

(6) IPSec 第二层隧道 VPN

一种通过隧道实现 PPP 帧跨互连网传输的过程，通过 IPSec 实现经过隧道传输的数据的保密性和完整性的 VPN。

(7) SSL VPN

一种基于 HTTPS 实现远程终端访问内部网络资源过程的 VPN。

(8) L2TP

一种动态建立基于 Internet 的第二层隧道或虚拟线路的信令协议。

(9) LAC

一种 ISP 接入控制设备，允许多个远程终端同时通过接入网络建立与该 ISP 接入控制设备之间的传输通路，并通过该 ISP 接入控制设备接入内部网络。

(10) LNS

内部网络连接 Internet 的接入控制设备。

第 11 章 防　火　墙

11.1 例题解析

11.1.1 简答题解析

【例题 11.1】 简述无状态分组过滤器控制网络间数据传输的过程。

【解析】 定义一个由一组规则组成的分组过滤器,规则指定了正常转发和丢弃的 IP 分组类型,将该分组过滤器作用于路由器接口的输入或输出方向,当某个 IP 分组需要从该路由器接口输入或输出时,依照顺序和该分组过滤器中的规则逐个匹配,一旦和某个规则匹配,则对该 IP 分组施加规则指定的操作。

【例题 11.2】 简述有状态分组过滤器控制网络间数据传输的过程。

【解析】 一般需要定义分组过滤器和监测机制,然后将分组过滤器和监测机制作用于路由器接口的输入或输出方向,一旦某个 IP 分组需要从该路由器接口输入或输出,首先和该路由器已经建立的会话匹配,如果该 IP 分组和某个已经建立的会话匹配,则直接转发该 IP 分组。否则,和同方向的分组过滤器进行匹配操作,如果匹配的结果是允许正常转发,且该 IP 分组的净荷是监测机制指定的传输层或应用层协议的协议数据单元,则创建对应会话。会话通常是用于传输应用层消息的 TCP 连接,当然也可以是两个 UDP 进程之间的数据交换过程,或是一次 ICMP ECHO 请求和响应过程。

和无状态分组过滤器不同,一是只有在该 IP 分组没有和路由器已经建立的会话匹配的情况下,才需要和该 IP 分组相同传输方向的分组过滤器进行匹配操作,并对该 IP 分组施加匹配规则指定的操作。二是一旦该 IP 分组与相同传输方向的分组过滤器匹配操作的结果是正常转发,且该 IP 分组的净荷是监测机制指定的传输层或应用层协议的协议数据单元,则创建对应会话。创建会话后,两个传输方向所有属于该会话的 IP 分组将直接转发,这些 IP 分组的转发操作与两个方向配置的分组过滤器无关。

【例题 11.3】 简述两个特定终端之间传输的 IP 分组和两个特定用户之间传输的 IP 分组的区别。

【解析】 为了确定某个 IP 分组的发送和接收用户,首先需要鉴别用户身份,在鉴别用户身份的过程中建立该用户与 IP 地址之间的绑定关系,这种绑定关系是动态的,因为同一用户可以通过不同的终端发送和接收数据。在该用户与 IP 地址之间的绑定关系存在期间,可以通过检测源和目的 IP 地址是否是该用户绑定的 IP 地址确定该 IP 分组是否由该用户发送或接收。为了防止源 IP 地址欺骗,有时需要通过安全协议 AH 保证 IP 分

组传输过程中的完整性。

11.1.2　设计题解析

【例题 11.4】 网络结构如图 11.1 所示，如果要禁止 LAN 1 和 LAN 2 之间的信息传输过程，如何在路由器中设置无状态分组过滤器？如果只允许 LAN 1 内终端访问 LAN 2 内的 Web 服务器，禁止其他信息的传输过程，如何在路由器中设置无状态分组过滤器？

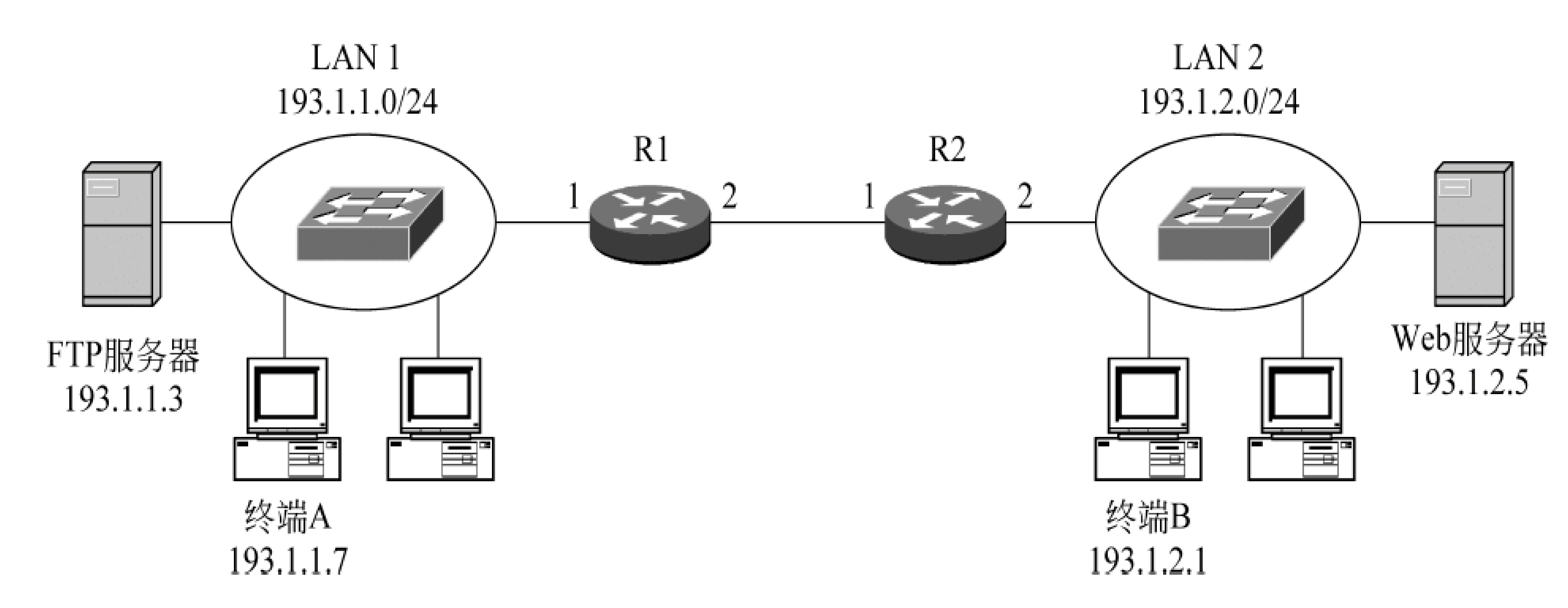


图 11.1　互连网结构

【解析】

(1) 如果要禁止 LAN 1 和 LAN 2 之间的信息传输过程，路由器 R1 接口 1 输入方向配置如表 11.1 所示的分组过滤器。输出方向配置如表 11.2 所示的分组过滤器。

同样，路由器 R2 接口 2 输入方向配置如表 11.3 所示的分组过滤器，输出方向配置如表 11.4 所示的分组过滤器。

表 11.1　路由器 R1 接口 1 输入方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	*	193.1.1.0/24	193.1.2.0/24	_	_	拒绝
2	*	*	*	_	_	允许

注：* 表示任意，_表示没有该项配置，后同。

表 11.2　路由器 R1 接口 1 输出方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	*	193.1.2.0/24	193.1.1.0/24	_	_	拒绝
2	*	*	*	_	_	允许

表 11.3　路由器 R2 接口 2 输入方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	*	193.1.2.0/24	193.1.1.0/24	_	_	拒绝
2	*	*	*	_	_	允许

表 11.4　路由器 R2 接口 2 输出方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	*	193.1.1.0/24	193.1.2.0/24	_	_	拒绝
2	*	*	*	_	_	允许

(2) 如果只允许 LAN 1 内终端访问 LAN 2 内的 Web 服务器，禁止其他信息的传输过程，路由器 R1 接口 1 输入方向配置如表 11.5 所示的分组过滤器，输出方向配置如表 11.6 所示的分组过滤器。

同样，路由器 R2 接口 2 输入方向配置如表 11.7 所示的分组过滤器，输出方向配置如表 11.8 所示的分组过滤器。

表 11.5　路由器 R1 接口 1 输入方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	193.1.1.0/24	193.1.2.5/32	＞1023	80	允许
2	*	*	*	_	_	拒绝

表 11.6　路由器 R1 接口 1 输出方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	193.1.2.5/32	193.1.1.0/24	80	＞1023	允许
2	*	*	*	_	_	拒绝

表 11.7　路由器 R2 接口 2 输入方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	193.1.2.5/32	193.1.1.0/24	80	＞1023	允许
2	*	*	*	_	_	拒绝

表 11.8　路由器 R2 接口 2 输出方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	193.1.1.0/24	193.1.2.5/32	＞1023	80	允许
2	*	*	*	_	_	拒绝

【例题 11.5】 对于如图 11.1 所示的网络，如果安全策略是"只允许经过路由器传输与终端 A 访问 Web 服务器、终端 B 访问 FTP 服务器操作有关的 IP 分组，禁止经过路由器传输其他一切类型的 IP 分组"，给出路由器 R1 和 R2 实现上述安全策略的有状态分组过滤器配置。

【解析】 路由器 R1 接口 1 输入方向配置的分组过滤器如表 11.9 所示，只允许与终端 A 发起访问 Web 服务器的过程相关的 IP 分组通过。输出方向配置的分组过滤器如表 11.10 所示，只允许与终端 B 发起访问 FTP 服务器的过程相关的 IP 分组通过。初始

状态下，路由器 R1 接口 1 输入方向禁止 FTP 服务器传输给终端 B 的 IP 分组通过，输出方向禁止 Web 服务器传输给终端 A 的 IP 分组通过。

路由器 R2 接口 2 输入输出方向配置的分组过滤器分别如表 11.11 和表 11.12 所示，其作用与路由器 R1 接口 1 输入输出方向配置的分组过滤器相似。

为了保证在终端 A 向 Web 服务器发送 HTTP 请求消息后，允许路由器 R1 接口 1 输出方向输出该 HTTP 请求消息对应的响应消息。需要在路由器 R1 接口 1 输入方向设置针对应用层协议 HTTP 的监测器，一旦路由器 R1 接口 1 输入方向监测到终端 A 发送给 Web 服务器的 HTTP 请求消息，则在路由器 R1 接口 1 输出方向动态生成允许该 HTTP 请求消息对应的响应消息通过的过滤规则。同样，需要在路由器 R1 接口 1 输出方向设置针对应用层协议 FTP 的监测器。

表 11.9　路由器 R1 接口 1 输入方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	193.1.1.7/32	193.1.2.5/32	>1023	80	允许
2	*	*	*	_	_	拒绝

表 11.10　路由器 R1 接口 1 输出方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	193.1.2.1/32	193.1.1.3/32	>1023	21	允许
2	TCP	193.1.2.1/32	193.1.1.3/32	>1023	20	允许
3	*	*	*	_	_	拒绝

表 11.11　路由器 R2 接口 2 输入方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	193.1.2.1/32	193.1.1.3/32	>1023	21	允许
2	TCP	193.1.2.1/32	193.1.1.3/32	>1023	20	允许
3	*	*	*	_	_	拒绝

表 11.12　路由器 R2 接口 2 输出方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	193.1.1.7/32	193.1.2.5/32	>1023	80	允许
2	*	*	*	_	_	拒绝

【例题 11.6】　网络结构如图 11.2 所示，内部网络被分成 5 个网络（VLAN 1～VLAN 5），分别分配网络地址 200.1.1.0/24、200.1.2.0/24、200.1.3.0/24、200.1.4.0/24 和 200.1.5.0/24，请制定符合下列安全策略的访问控制策略，并根据访问控制策略解释防火墙阻止属于 VLAN 3 的终端访问非军事区中的服务器的工作机制。

- 允许属于 VLAN 1 的终端访问内部网络服务器、非军事区中的服务器和 Internet

中的 Web 和 FTP 服务器。

- 允许属于 VLAN 2 的终端访问内部网络服务器和非军事区中的 Web 服务器。
- 允许属于 VLAN 3 的终端访问内部网络服务器。

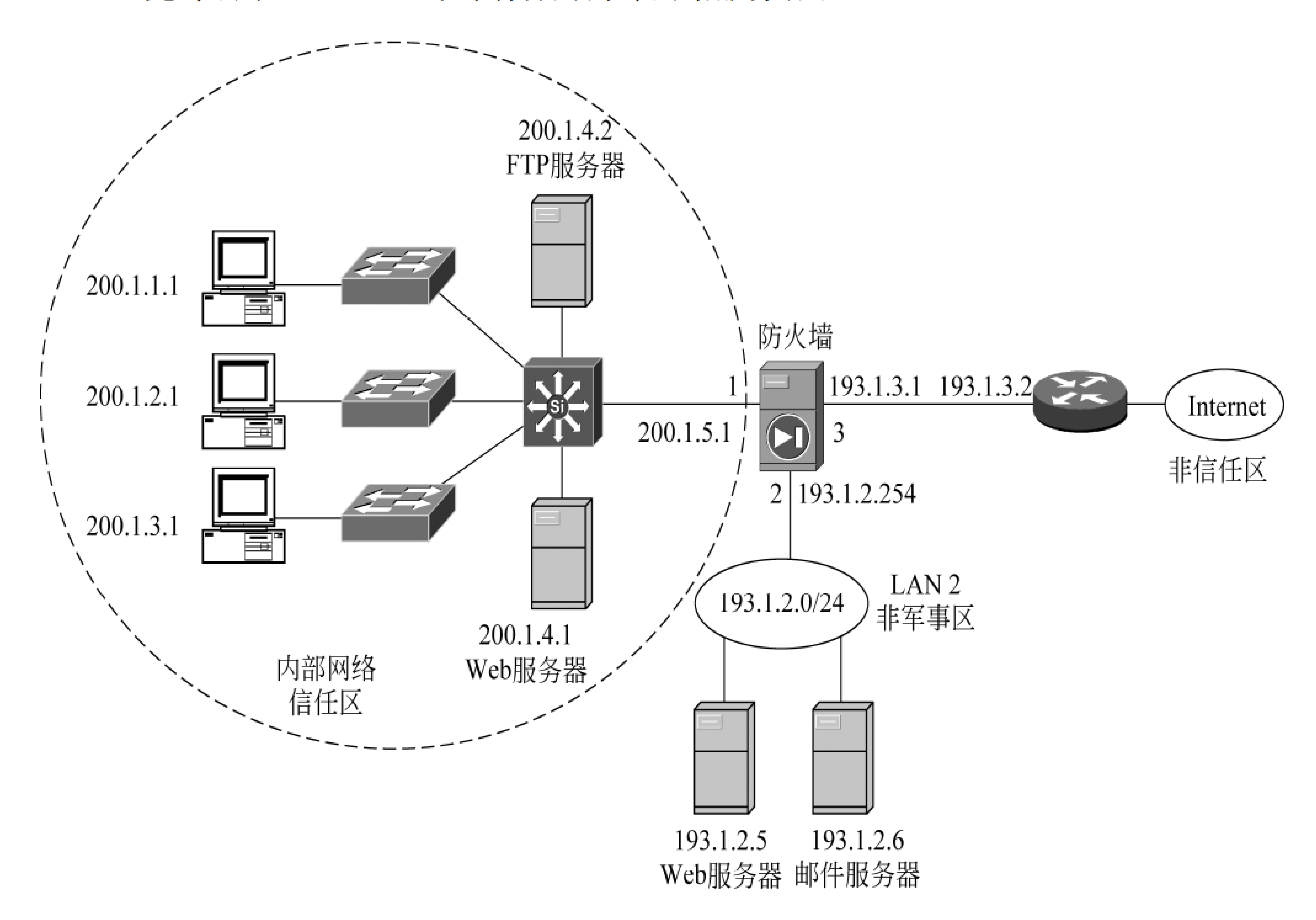


图 11.2 网络结构

【解析】 防火墙配置的访问控制策略如表 11.13 所示。如果属于 VLAN 3 的终端发起访问非军事区中的服务器的过程,属于 VLAN 3 的终端发送一个源 IP 地址为 200.1.3.0/24、目的 IP 地址为 193.1.2.5/32 或者 193.1.2.6/32 的 IP 分组,当防火墙通过接口 1 接收到该 IP 分组,根据 IP 分组的目的 IP 地址检索路由表,确定通过接口 2 转发该 IP 分组,由于接口 1 绑定信任区、接口 2 绑定非军事区,在表 11.13 所示的访问控制策略中检索信息流动方向为从信任区到非军事区,源 IP 地址=200.1.3.0/24,目的 IP 地址为 193.1.2.5/32 或者 193.1.2.6/32 的访问控制策略。由于表 11.13 所示的访问控制策略中不存在符合上述条件的访问控制策略,因此防火墙丢弃该 IP 分组。

表 11.13 防火墙配置的访问控制策略

信息流动方向	源 IP 地址	目的 IP 地址	服务
从信任区到非军事区	200.1.1.0/24	193.1.2.5/32	HTTP
从信任区到非军事区	200.1.1.0/24	193.1.2.6/32	SMTP+POP3
从信任区到非军事区	200.1.2.0/24	193.1.2.5/32	HTTP
从信任区到非信任区	200.1.1.0/24	*	HTTP+FTP

【例题 11.7】 对于如图 11.3 所示的网络结构,列出四种实现远程终端访问内部网络 Web 服务器过程的方法,给出实现远程访问过程需要的配置,并比较这四种方法的优

缺点。

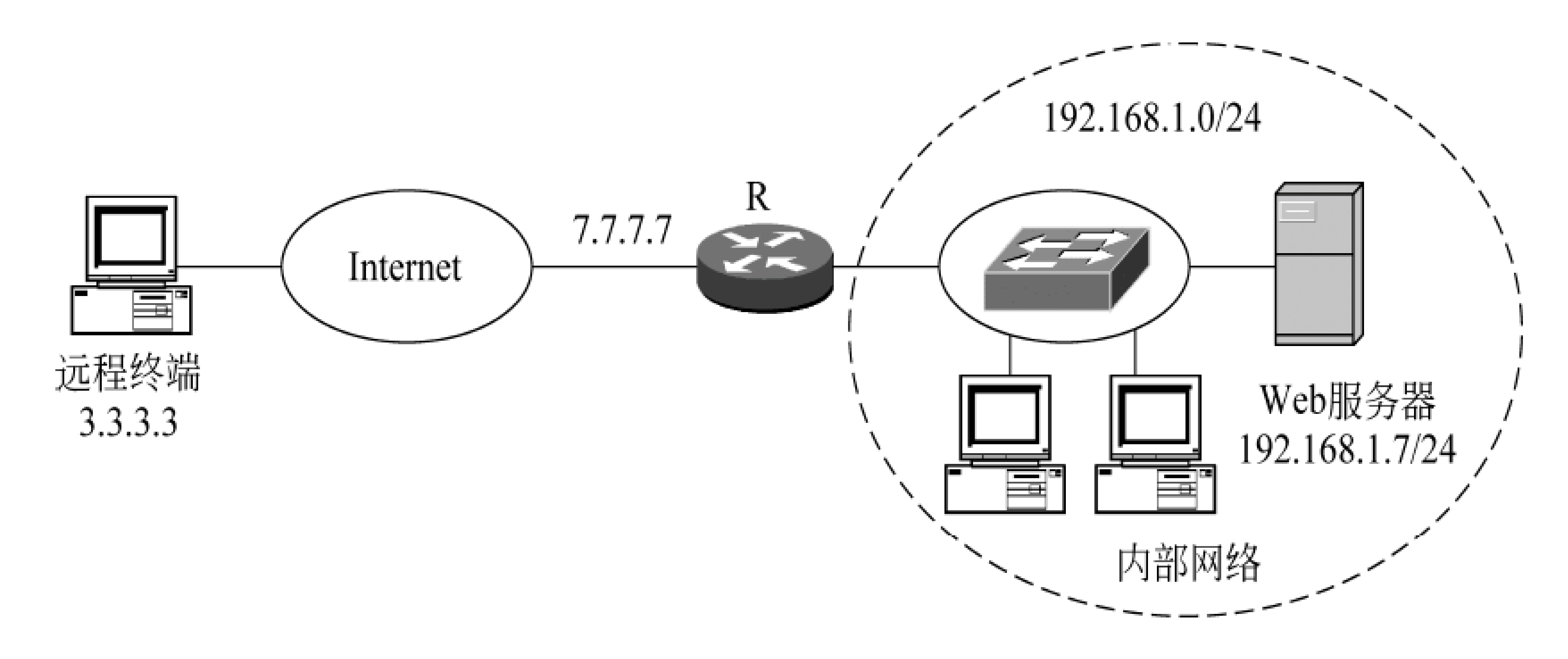


图11.3　网络结构

【解析】

(1) 静态端口映射

静态配置全局端口号80与Web服务器私有IP地址192.168.1.7之间的映射，在路由器R中建立如表11.14所示的地址转换表，远程终端可以通过IP地址7.7.7.7和端口号80访问Web服务器。

表11.14　路由器R地址转换表

协　议	Inside Local	Inside Global
TCP	192.168.1.7:80	7.7.7.7:80

(2) 第二层隧道VPN

路由器R作为LNS，远程终端通过第二层隧道VPN接入内部网络，分配私有IP地址，然后像内部网络终端一样访问Web服务器。

① 远程终端配置信息

第二层隧道控制协议：L2TP。

LNS地址：7.7.7.7。

用户名：用户A。

密码：PASSA。

鉴别协议：CHAP。

② LNS配置信息

第二层隧道控制协议：L2TP。

本地IP地址池：192.168.2.1～192.168.2.100。

注册用户库如表11.15所示。

表11.15　注册用户库

用　户　名	密　　码	鉴别协议
用户A	PASSA	CHAP

③ 远程接入用户访问企业内部网络资源的过程

- 通过 L2TP 建立远程终端与 LNS 之间的第二层隧道。
- 远程终端与 LNS 之间建立基于第二层隧道的 PPP 链路。
- LNS 完成对远程终端用户的身份鉴别过程。
- LNS 在本地 IP 地址池中选择一个未使用的本地 IP 地址(如 192.168.2.1),将其分配给远程终端,并在路由表中创建一项将该本地 IP 地址和远程终端与 LNS 之间的第二层隧道绑定在一起的路由项。
- 远程终端用 LNS 分配的本地 IP 地址,像企业内部网络中的终端一样访问企业内部网络资源。

(3) SSL VPN

路由器 R 具备 SSL VPN 网关功能。

① SSL VPN 网关完成证书申请过程,远程终端获取证明 SSL VPN 网关的 IP 地址 7.7.7.7 与其公钥之间绑定关系的证书。

② SSL VPN 网关配置如表 11.16 所示的注册用户库,注册用户库中列出所有注册用户的用户名和密码。

③ 为每一个注册用户分配访问权限,建立如表 11.17 所示的用户权限表。用户权限用该注册用户能够访问的对象表示,每一个对象用 URL 唯一标识。用 URL=192.168.1.7 标识 Web 服务器主页。

④ 每一个注册用户可以登录 SSL VPN 网关,成功登录后,给出 URL 列表,URL 列表中是一组标识授权该注册用户访问的对象的 URL。

表 11.16 注册用户库

用户名	密　码
用户 A	PASSA

表 11.17 用户权限表

用户名	访 问 权 限
用户 A	URL=http://192.168.1.7

(4) 电路层网关

路由器 R 作为电路层网关,配置如表 11.18 所示的授权用户库和如表 11.19 所示的用户权限表。远程终端首先建立与路由器 R 之间的 TCP 连接,然后由路由器 R 完成对远程用户的身份鉴别过程。最后由远程终端向路由器 R 发出请求建立与 Web 服务器之间的 TCP 连接的请求,由于用户权限表中表明用户 A 具有建立与私有 IP 地址为 192.168.1.7 的 Web 服务器之间的 TCP 连接的权限,路由器 R 建立与 Web 服务器之间的 TCP 连接,并建立如表 11.20 所示的远程终端与路由器 R 之间的 TCP 连接和路由器 R 与 Web 服务器之间的 TCP 连接之间的映射。其中 192.168.1.1 是路由器 R 连接内部网络的接口的私有 IP 地址。

表 11.18 授权用户库

用户名	密码
用户 A	PASSA

表 11.19 用户权限表

用户名	访 问 权 限	
	传输层协议	目的端插口
用户 A	TCP	192.168.1.7:80

表 11.20　TCP 连接映射表

远程终端与路由器 R 之间的 TCP 连接		路由器 R 与 Web 服务器之间的 TCP 连接	
终端插口	路由器 R 插口	路由器 R 插口	Web 服务器插口
3.3.3.3:1273	7.7.7.7:1080	192.168.1.1:2373	192.168.1.7:80

(5) 四种方法比较分析

① 透明性

SSL VPN 网关和静态端口映射方法下，内部网络 Web 服务器对于远程终端是透明的。电路层代理和第二层隧道 VPN 方法下，远程终端需要知道内部网络 Web 服务器的私有 IP 地址。

② 可控制性

SSL VPN 网关、静态端口映射和电路层代理都可将远程终端对内部网络的访问权限严格控制为只对 Web 服务器的访问。第二层隧道 VPN 如果没有与其他安全机制相结合，远程终端可以像内部网络终端一样访问内部网络资源。

③ 安全性

SSL VPN 和第二层隧道 VPN 可以保证远程终端与路由器 R 之间传输信息的保密性和完整性，但静态端口映射和电路层代理没有这一功能。

④ 方便性

远程终端可以用标准浏览器实现 SSL VPN 网关、静态端口映射和电路层代理方法下对内部网络 Web 服务器的访问过程。但远程终端需要专用客户端软件实现第二层隧道 VPN 方法下对内部网络 Web 服务器的访问过程。

【例题 11.8】 双重宿主主机体系结构如图 11.4 所示，其中的堡垒主机是电路层代理，用于控制远程终端对内部网络 Web 服务器的访问过程。给出实现上述功能的堡垒主机的配置。

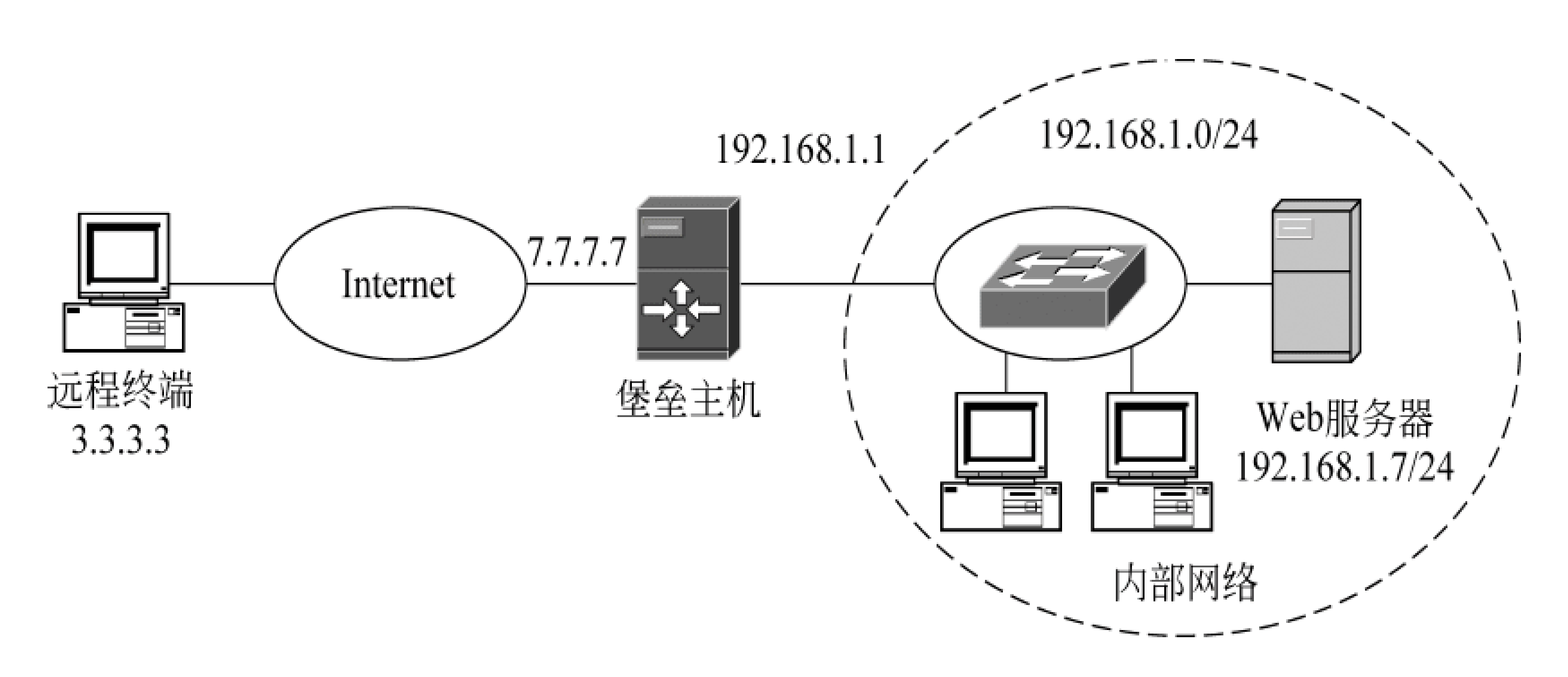


图 11.4　双重宿主主机体系结构

【解析】 双重宿主主机体系结构中的堡垒主机如图 11.4 所示，存在两个网络接口，一个网络接口用于连接 Internet，另一个网络接口用于连接内部网络。远程终端可以通过堡垒主机连接 Internet 接口的 IP 地址访问堡垒主机。内部网络对于远程终端是透明的。但内部网络中的 Web 服务器对于授权用户不是透明的。堡垒主机中需要配置如

表 11.21 所示的授权用户库,授权用户库中给出所有授权用户的用户名和密码。同时,还需配置如表 11.22 所示的用户权限表,用户权限表针对每一个授权用户给出该授权用户允许访问的服务器,以及访问该服务器时使用的传输层协议。

表 11.21 授权用户库

用户名	密码
用户 A	PASSA
用户 B	PASSB

表 11.22 用户权限表

用户名	访问权限	
	传输层协议	目的端插口
用户 A	TCP	192.168.1.7:80
用户 B	TCP	192.168.1.7:80

完成上述配置后,授权用户可以通过 URL=http://7.7.7.7:1080 登录堡垒主机,堡垒主机完成对授权用户的身份鉴别过程后,作为代理建立与内部网络 Web 服务器之间的 TCP 连接,然后,建立远程终端与堡垒主机之间的 TCP 连接和堡垒主机与内部网络 Web 服务器之间 TCP 连接的映射。

【例题 11.9】 被屏蔽主机体系结构如图 11.5 所示,其中的堡垒主机是电路层代理,用于控制远程终端对内部网络 Web 服务器的访问过程。给出实现上述功能的堡垒主机和路由器 R 的配置。

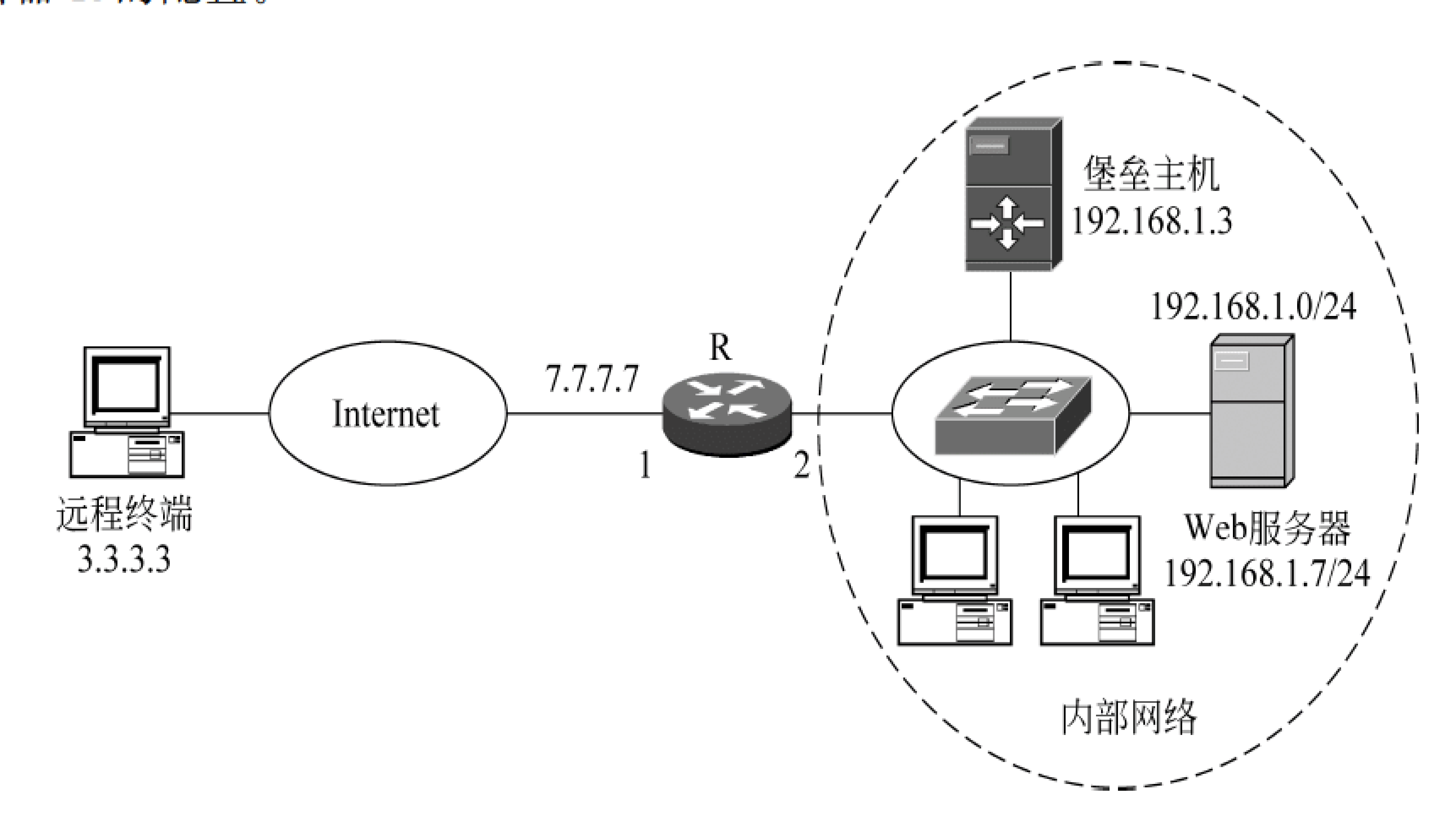


图 11.5 被屏蔽主机体系结构

【解析】 由于内部网络对于远程终端是透明的,因此,路由器 R 需要配置如表 11.23 所示的静态地址转换表,地址转换表中建立 7.7.7.7:1080 和 192.168.1.3:1080 之间的映射。为了保证远程终端只能访问到内部网络中的堡垒主机,路由器 R 接口 2 输入/输出方向分别配置表 11.24 和表 11.25 所示的分组过滤器。堡垒主机中配置的授权用户库和用户权限表如表 11.21 和表 11.22 所示。

表 11.23 路由器 R 地址转换表

协 议	Inside Local	Inside Global
TCP	192.168.1.3:1080	7.7.7.7:1080

表 11.24 路由器 R 接口 2 输入方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	192.168.1.3/32	*	1080	>1023	允许
2	*	*	*	_	_	拒绝

表 11.25 路由器 R 接口 2 输出方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	*	192.168.1.3/32	>1023	1080	允许
2	*	*	*	_	_	拒绝

完成上述配置后，授权用户可以通过 URL=http://7.7.7.7:1080 登录堡垒主机，堡垒主机完成对授权用户的身份鉴别过程后，作为代理建立与内部网络 Web 服务器之间的 TCP 连接，然后，建立远程终端与堡垒主机之间的 TCP 连接和堡垒主机与内部网络 Web 服务器之间 TCP 连接的映射。

【例题 11.10】 被屏蔽子网体系结构如图 11.6 所示，路由器 R1 和 R2 之间的网络是非军事区。其中的堡垒主机是电路层代理，用于控制远程终端对内部网络 Web 服务器的访问过程。要求远程终端只能访问非军事区中的堡垒主机、Web 服务器和邮件服务器，不能直接访问内部网络。给出实现上述功能的堡垒主机和路由器 R1、R2 的配置。

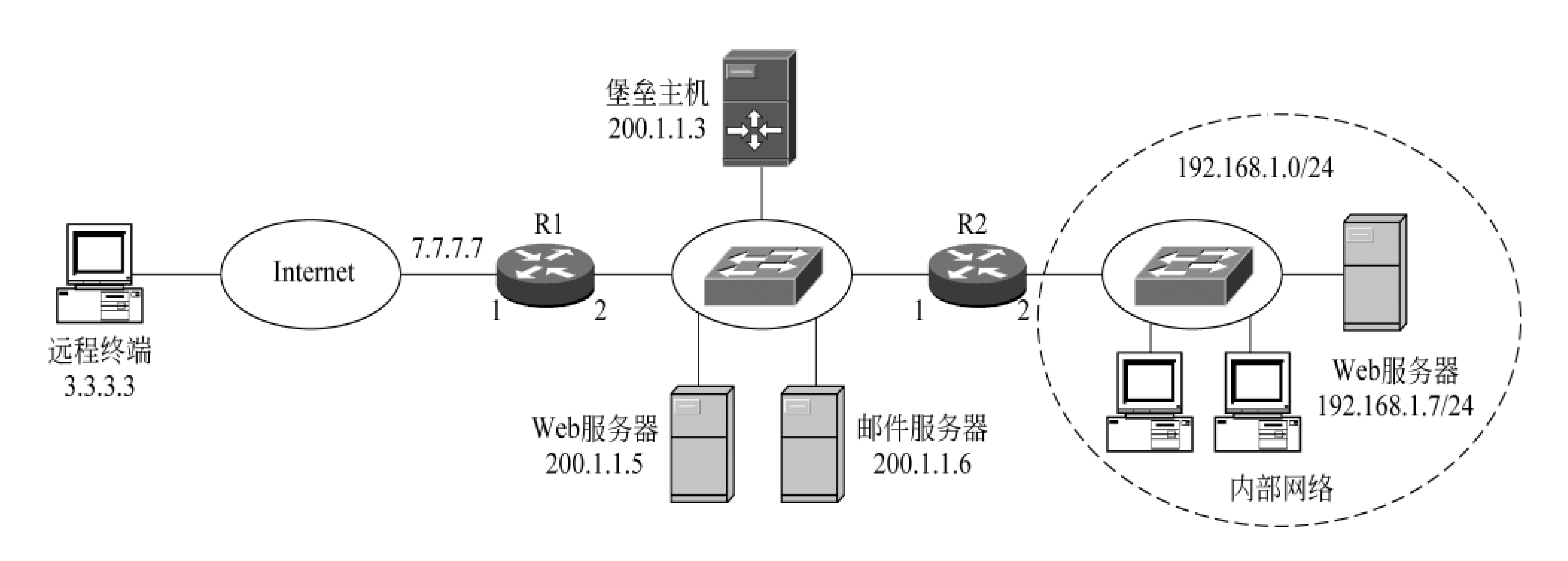


图 11.6 被屏蔽子网体系结构

【解析】 路由器 R1 接口 2 输出/输入方向分别配置如表 11.26 和表 11.27 所示的分组过滤器，保证远程终端只能访问到非军事区中的堡垒主机、Web 服务器和邮件服务器。假定路由器 R2 接口 1 的 IP 地址是 200.1.1.7，由于内部网络对于远程终端和非军事区都是透明的，因此，路由器 R2 需要配置如表 11.28 所示的静态地址转换表，地址转换表中建立 200.1.1.7:80 和 192.168.1.7:80 之间的映射。

为了保证只允许由非军事区中的堡垒主机发起访问内部网络中的 Web 服务器的过程，路由器 R2 接口 2 输出/输入方向分别配置如表 11.29 和表 11.30 所示的分组过滤器。堡垒主机需要配置表 11.21 所示的授权用户库和表 11.31 所示的用户权限表。

表 11.26　路由器 R1 接口 2 输出方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	*	200.1.1.5/32	>1023	80	允许
2	TCP	*	200.1.1.6/32	>1023	25	允许
3	TCP	*	200.1.1.6/32	>1023	110	允许
4	TCP	*	200.1.1.3/32	>1023	1080	允许
5	*	*	*	_	_	拒绝

表 11.27　路由器 R1 接口 2 输入方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	200.1.1.5/32	*	80	>1023	允许
2	TCP	200.1.1.6/32	*	25	>1023	允许
3	TCP	200.1.1.6/32	*	110	>1023	允许
4	TCP	200.1.1.3/32	*	1080	>1023	允许
5	*	*	*	_	_	拒绝

表 11.28　R2 地址转换表

协　议	Inside Local	Inside Global
TCP	192.168.1.7：80	200.1.1.7：80

表 11.29　路由器 R2 接口 2 输出方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	200.1.1.3/32	192.168.1.7/32	>1023	80	允许
2	*	*	*	_	_	拒绝

表 11.30　路由器 R2 接口 2 输入方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	192.168.1.7/32	200.1.1.3/32	80	>1023	允许
2	*	*	*	_	_	拒绝

表 11.31　用户权限表

用户名	访 问 权 限	
	传输层协议	目的端插口
用户 A	TCP	200.1.1.7:80
用户 B	TCP	200.1.1.7:80

完成上述配置后，授权用户可以通过 URL＝http：//200.1.1.3：1080 登录堡垒主机，堡垒主机完成对授权用户的身份鉴别过程后，作为代理建立与内部网络 Web 服务器之间的 TCP 连接，然后，建立远程终端与堡垒主机之间的 TCP 连接和堡垒主机与内部网络 Web 服务器之间 TCP 连接的映射。

【例题 11.11】 分析双重宿主主机体系结构、被屏蔽主机体系结构和被屏蔽子网体系结构的安全性。

【解析】 对于双重宿主主机体系结构，堡垒主机直接暴露在 Internet 中，所有远程终端可以访问堡垒主机，因此，内部网络 Web 服务器的安全完全取决于堡垒主机的安全。

对于被屏蔽主机体系结构，连接 Internet 和内部网络的边界路由器 R 可以通过分组过滤器控制远程终端对堡垒主机的访问过程，增加了远程终端攻击堡垒主机的难度。

对于被屏蔽子网体系结构，连接 Internet 和非军事区的边界路由器 R1 可以通过分组过滤器控制远程终端对堡垒主机的访问过程，连接非军事区和内部网络的边界路由器 R2 可以通过分组过滤器控制堡垒主机对内部网络 Web 服务器的访问过程。因此，被屏蔽子网体系结构是三种防火墙体系结构中对内部网络 Web 服务器保护最严格的防火墙体系结构。

11.2 选择题分析

(1) 关于防火墙，以下哪一项描述是错误的？(　　)

A. 阻断有害信息从一个网络进入另一个网络

B. 阻断有害信息进入终端

C. 对网络之间进行的信息交换过程实施控制

D. 对网络设备实施物理保护

答案：D

【分析】 网络安全范畴中的防火墙不是一堵用于对网络设备实施物理保护的墙，而是一种对网络之间，或者网络与终端之间进行的信息交换过程实施控制的装置。

(2) 以下哪一项不属于网络防火墙的类型？(　　)

A. 分组过滤器　　B. 电路层代理

C. 应用层网关　　D. 堡垒主机

答案：D

【分析】 堡垒主机是一种被强化的可以防御进攻的计算机，安装软件防火墙后，也可作为防火墙使用。根据安装的软件防火墙功能的不同，堡垒主机可以作为分组过滤器、电路层代理和应用层网关。因此，堡垒主机本身不属于网络防火墙类型。

(3) 关于防火墙，以下哪一项描述是错误的？(　　)

A. 不能防范内网内的恶意攻击

B. 不能防范针对面向连接协议的攻击

C. 不能防范病毒和内部驱动的木马

D. 不能防范针对防火墙开放端口的攻击

答案：B

【分析】 有状态分组过滤器可以有效防范针对面向连接协议的攻击。

(4) 关于无状态分组过滤器，以下哪一项描述是错误的？(　　)

A. 在 IP 分组流中过滤掉具有特定属性的一组 IP 分组

B. 属性通常包括源和目的 IP 地址、源和目的端口号

C. 实施筛选和控制操作时，每一个 IP 分组都是独立的

D. 控制两个特定用户之间的信息传输过程

答案：D

【分析】 可以通过源和目的 IP 地址确定两个终端，也可以通过源和目的端口号确定两个进程，但一般无法根据 IP 分组携带的属性确定两个用户。

(5) 关于无状态分组过滤器，以下哪一项描述是错误的？(　　)

A. 无状态分组过滤器用于独立确定每一个 IP 分组是正常转发还是丢弃

B. 作用于一个方向的无状态分组过滤器只能控制该方向的 IP 分组传输过程

C. 无状态分组过滤器只能检测 IP 首部字段

D. 两个方向上设置的无状态分组过滤器独立控制对应方向上的 IP 分组传输过程

答案：C

【分析】 无状态分组过滤器不但检测 IP 首部字段，还检测传输层首部字段。

(6) 关于无状态分组过滤器，以下哪一项描述是错误的？(　　)

A. 能够控制两个不同网络之间的数据传输过程

B. 能够控制两个终端之间的数据传输过程

C. 能够控制两个进程之间的数据传输过程

D. 能够控制一次完整应用所涉及的数据交换过程

答案：D

【分析】 这是有状态分组过滤器才具有的功能。

(7) 关于规则，以下哪一项描述是错误的？(　　)

A. 过滤器可以由多项规则组成

B. 根据规则顺序逐项匹配

C. 只有和当前规则不匹配时，才和后续规则进行匹配操作

D. 匹配结果与过滤器中的规则顺序无关

答案：D

【分析】 由于 IP 分组只有和当前规则不匹配时，才继续和后续规则进行匹配操作，一旦和某个规则匹配，则对其进行规则指定的操作，不再和其他规则进行匹配操作。由于过滤器中的规则顺序决定 IP 分组匹配规则的顺序，因此，匹配结果与过滤器中的规则顺序有关。

(8) 关于过滤器和接口输入/输出方向，以下哪一项描述是错误的？(　　)

A. 过滤器可以作用于接口的输入方向或输出方向

B. 从接口输入的 IP 分组匹配作用于输入方向的过滤器

C. 从接口输出的 IP 分组匹配作用于输出方向的过滤器

D. 同一过滤器不能同时作用于接口的输入和输出方向

答案：D

【分析】 同一过滤器可以同时作用于接口的输入和输出方向。

(9) 关于无状态分组过滤器,以下哪一项描述是错误的？(　　)

A. 阻止两个终端之间的通信过程　　B. 阻止两个进程之间的通信过程

C. 阻止两个用户之间的通信过程　　D. 阻止两个网络之间的通信过程

答案：C

【分析】 可以通过源和目的 IP 地址属性指定两个终端或两个网络,可以通过源和目的端口号属性指定两个进程,但无法指定两个用户。

(10) 关于有状态分组过滤器,以下哪一项描述是错误的？(　　)

A. 基于会话控制通信过程

B. 属于同一会话的 IP 分组之间存在关联

C. 对 IP 分组的操作与会话的状态有关

D. 存在显式的会话建立和删除过程

答案：D

【分析】 类似 UDP 会话和 ICMP ECHO 请求和响应过程不存在显式的会话建立和删除过程。

(11) 关于有状态分组过滤器,以下哪一项描述是错误的？(　　)

A. 创建会话时匹配过滤规则

B. 允许属于指定会话的 TCP 报文传输

C. TCP 连接是一次会话过程

D. 配置有状态分组过滤器时静态创建对应会话

答案：D

【分析】 会话是动态创建的,当扩展分组过滤器允许某个 IP 分组正常转发且该 IP 分组的净荷是监测机制指定的应用层或传输层协议的协议数据单元时,创建会话。

(12) 关于有状态分组过滤器,以下哪一项描述是正确的？(　　)

A. 需要分别作用于接口输入和输出方向的两个独立过滤器

B. 接口允许输入和输出的 IP 分组是相互独立的

C. 对输入和输出 IP 分组实施操作的唯一依据是输入/输出方向作用的分组过滤器

D. 用分组过滤器控制会话建立过程,基于会话状态对属于该会话的 IP 分组实施操作

答案：D

【分析】 对于有状态分组过滤器,作用于接口的分组过滤器只适用于控制会话建立过程,建立会话后,基于会话状态对属于该会话的 IP 分组实施操作。这是有状态分组过滤器区别于无状态分组过滤器的地方。

(13) 关于有状态分组过滤器的会话,以下哪一项描述是错误的?( )

A. 一个 TCP 连接

B. 两个进程之间的 UDP 报文传输过程

C. 一次 ICMP ECHO 请求和响应过程

D. 访问网站过程

答案:D

【分析】 访问网站可能涉及多个会话,如域名解析过程就有可能涉及多次 UDP 报文交换过程。

(14) 关于有状态分组过滤器,以下哪一项描述是错误的?( )

A. 有状态分组过滤器用于控制基于特定应用的数据交换过程

B. 有状态分组过滤器同时控制两个方向上的 IP 分组传输过程

C. 有状态分组过滤器两个方向上的 IP 分组传输控制机制存在相互制约

D. 有状态分组过滤器能控制两个特定用户之间的数据交换过程

答案:D

【分析】 有状态分组过滤器不具有身份鉴别功能,无法确定数据的发送和接收用户。

(15) 关于应用层有状态分组过滤器,以下哪一项描述是错误的?( )

A. 用分组过滤器控制会话建立过程

B. 基于会话状态和应用层协议规范对属于该会话的 IP 分组实施操作

C. 检测应用层请求消息与响应消息之间的关联性

D. 会话可以是多个 TCP 连接

答案:D

【分析】 对于应用层有状态分组过滤器,会话还是一个 TCP 连接,或是两个进程之间的 UDP 报文传输过程,只是增加了基于特定应用层的协议规范,对 TCP 报文或 UDP 报文中的净荷进行深度检测的功能。

(16) 有状态分组过滤器基于会话或服务实施控制,以下哪一项对会话或服务的描述是错误的?( )

A. 会话是包括建立、通信和释放的一次完整 TCP 连接

B. 会话是有限时间内两个 UDP 进程之间的数据传输过程

C. HTTP 服务是一次完整的 Web 服务器访问过程

D. 邮件服务是一次发送和接收邮件的过程

答案:D

【分析】 发送邮件和接收邮件是两个独立的服务。

(17) 以下哪一项是有状态分组过滤器和无状态分组过滤器之间的主要区别?( )

A. 对分组实施的操作有丢弃和正常转发

B. 每一个分组独立地根据与过滤规则的匹配结果确定对其施加的操作

C. 位于网络间数据传输通路上

D. 根据安全策略控制网络间的数据交换过程

答案:B

【分析】 这是无状态分组过滤器有别于有状态分组过滤器的特性。

(18) 关于基于分区防火墙，以下哪一项描述是错误的？(　　)

A. 控制区间通信过程

B. 用服务定义信息交换过程

C. 可以定义服务发起端范围和服务响应端范围

D. 服务定义的信息交换过程只涉及应用层消息的传输过程

答案：D

【分析】 服务定义的信息交换过程包括用于传输应用层消息的会话的建立和删除过程，如 FTP 服务，涉及 TCP 控制连接和 TCP 数据连接的建立和删除过程。

(19) 关于电路层代理，以下哪一项描述是错误的？(　　)

A. 用于解决无法建立 TCP 连接或 UDP 会话的源主机和目的主机之间的通信过程

B. 可以对源主机用户实施身份鉴别

C. 建立源主机用户和源主机与电路层网关之间的 TCP 连接或 UDP 会话之间的绑定

D. 电路层网关通过 PAT 实现源主机和目的主机之间的通信过程

答案：D

【分析】 电路层网关通过建立源主机与电路层网关之间的 TCP 连接或 UDP 会话和电路层网关与目的主机之间的 TCP 连接或 UDP 会话之间的映射实现源主机和目的主机之间的通信过程。

(20) 关于电路层代理，以下哪一项描述是错误的？(　　)

A. 建立源主机与电路层网关之间的 TCP 连接或 UDP 会话

B. 建立电路层网关与目的主机之间的 TCP 连接或 UDP 会话

C. 建立上述两个 TCP 连接或 UDP 会话之间的映射

D. 根据映射完成 TCP 或 UDP 报文之间的相互转换

答案：D

【分析】 电路层代理将通过源主机与电路层代理之间的 TCP 连接或 UDP 会话接收到的源主机发送的数据复制到电路层代理与目的主机之间的 TCP 连接或 UDP 会话，或者反之，将通过电路层代理与目的主机之间的 TCP 连接或 UDP 会话接收到的目的主机发送的数据复制到源主机与电路层代理之间的 TCP 连接或 UDP 会话。以此实现源主机和目的主机之间的通信过程。

(21) 关于电路层网关安全功能，以下哪一项描述是错误的？(　　)

A. 数据中继　　B. 用户身份鉴别

C. 传输层检测　　D. 地址转换

答案：D

【分析】 电路层网关不是通过地址转换完成数据中继过程的。

(22) 关于应用层网关，以下哪一项描述是错误的？(　　)

A. 针对特定应用层协议

B. 防御针对特定应用的攻击行为

C. 工作在透明模式或代理模式

D. 是一个集成在应用服务器中的软件模块

答案：D

【分析】 目前大量的应用层网关是一个独立的设备，可以同时保护多台提供特定网络服务的应用服务器。

(23) 关于 WAF，以下哪一项描述是错误的？(　　)

A. 检测 HTTP 消息各个字段值

B. 对 HTTP 消息进行攻击特征匹配

C. 应用规律统计分析

D. 用户身份鉴别

答案：D

【分析】 WAF 一般不负责用户授权，因此，WAF 不会进行用户身份鉴别。

(24) 下列选项中，哪一项不属于防火墙体系结构？(　　)

A. 双重宿主主机体系结构　　B. 被屏蔽主机体系结构

C. 被屏蔽子网体系结构　　D. 被屏蔽中间网络体系结构

答案：D

【分析】 防火墙体系结构分为双重宿主主机体系结构、被屏蔽主机体系结构和被屏蔽子网体系结构。

11.3 名词解释

(1) 防火墙

一种位于网络或者用户终端与网络之间，对网络或者网络与用户终端之间传输的信息流实施控制的设备。

(2) 个人防火墙

安装在主机中的软件防火墙，用于对用户终端与网络之间传输的信息流实施控制。

(3) 网络防火墙

位于两个网络之间，用于对网络之间传输的信息流实施控制的装置，这个装置可以是独立的设备，也可以集成在路由器中。

(4) 无状态分组过滤器

能够从一个网络进入另一个网络的全部 IP 分组中筛选出符合用户指定特征的一部分 IP 分组，并对这一部分 IP 分组的网络间传输过程实施控制。当实施筛选和控制操作时，每一个 IP 分组都是独立的，不考虑 IP 分组之间的关联性。

(5) 有状态分组过滤器

能够鉴别出属于同一会话的 IP 分组，然后根据会话的属性与状态对属于该会话的 IP 分组的网络间传输过程进行控制。

(6) 电路层代理

一个在源和目的主机之间无法直接建立 TCP 连接或 UDP 会话的情况下,用于实现源主机和目的主机之间的通信过程的中继设备。

(7) 应用层网关

一种能够对每一种网络服务,提供用于防御针对该网络服务的攻击行为的设备。

(8) 堡垒主机

一种被强化的、可以防御进攻的计算机,安装软件防火墙后,也可作为防火墙使用。根据安装的软件防火墙功能的不同,可以作为分组过滤器、电路层代理和应用层网关。

第12章 入侵检测系统

12.1 例题解析

12.1.1 简答题解析

【例题12.1】 简述产生入侵检测系统的原因。

【解析】 一种新技术的产生，通常基于以下两个原因：一是碰到已有技术无法解决的问题；二是找到解决这些问题的新方法。产生入侵检测系统的原因有以下四个：一是攻击信息无处不在，仅仅通过防火墙对网络间数据交换过程实施控制已无法阻止攻击信息扩散；二是攻击行为与正常访问过程之间存在差异，这种差异可以通过建立攻击特征库和描述正常访问过程的行为模式检测出来；三是可以通过建立资源访问控制列表，实施主机资源的授权访问，同时也可以通过资源访问控制列表检测出非法资源访问操作；四是交换机和路由器等网络设备既容易实现信息收集，又容易阻断攻击信息的传输过程。上述原因导致产生一种与交换机和路由器集成在一起或运行于主机系统，通过在网络关键节点或关键链路收集信息和分析信息，检测出非法访问操作、违反安全策略和入侵的行为，并对这些行为予以反制的设备。

【例题12.2】 简述网络入侵检测系统和防火墙的区别。

【解析】 一是检测的信息不同。防火墙只检测网络间传输的信息，入侵检测系统能够检测流经任何网段的信息。二是检测机制不同。防火墙根据配置的访问控制策略确定信息是否违反安全策略，并丢弃违反安全策略的信息。入侵检测系统根据建立的攻击特征库和描述正常访问过程的行为模式确定是否是攻击信息，并对攻击信息予以反制。三是作用不同。防火墙的作用是通过静态配置访问控制策略限制网络间允许交换的信息流类型。入侵检测系统通过分析已经发现的入侵行为，如蠕虫传播过程、木马窃取信息资源过程和黑客利用操作系统漏洞实施的攻击过程，提取出攻击特征，通过对这些攻击特征的匹配操作，可以检测出正在进行的攻击行为，并予以反制，因此，入侵检测系统的主要作用是阻止已知和未知的攻击行为继续。四是入侵检测系统可以通过在多个关键节点和关键链路收集信息，并对这些信息的检测结果进行综合分析发现分布式拒绝服务攻击，以及其他对网络的侦察行为。防火墙不具有这一功能。

【例题12.3】 简述主机入侵检测系统和网络入侵检测系统的区别。

【解析】 一是收集的信息不同。主机入侵检测系统只收集进出主机的信息。网络入侵检测系统收集流经任何网段的信息。二是作用不同。主机入侵检测系统主要用于阻止

对主机资源的非法操作。网络入侵检测系统能够阻止已知和未知的攻击行为继续，这些攻击行为包括蠕虫传播过程、木马窃取信息资源过程和黑客利用操作系统漏洞实施的攻击过程等。三是保护对象不同。网络入侵检测系统保护网段后面的多台主机、多段网段，甚至一个网络。主机入侵检测系统只保护单个主机系统。四是主机入侵检测系统能够截获有关用户、进程、访问对象、访问方式等信息，可以利用这些信息实施精确监控。网络入侵检测系统收集的与资源访问操作有关的信息没有主机入侵检测系统详细。五是主机入侵检测系统可以通过配置资源访问控制列表实施授权访问，网络入侵检测系统不具有这一功能。

【例题 12.4】 简述网络入侵检测系统的实现机制。

【解析】 一是收集信息。可以通过在线方式收集流经该链路的信息，也可以在杂凑方式下，通过和交换机或路由器等网络设备配合，收集经过这些网络设备转发的信息。二是需要建立攻击特征库，或是描述正常访问过程的行为模式。三是需要设计用于将收集的信息与建立的攻击特征库和描述正常访问过程的行为模式进行比较的匹配操作算法。四是需要设计针对攻击信息的反制动作。五是需要对已经发现的病毒传播过程、木马窃取信息资源过程和黑客利用操作系统漏洞实施的攻击过程进行分析，提取出攻击特征，及时添加到攻击特征库中。六是需要不断调整描述正常访问过程的行为模式，在误报和漏报间取得平衡。

【例题 12.5】 简述入侵检测系统防御黑客攻击的机制。

【解析】 一是通过分析黑客攻击的一般步骤，给出用于描述黑客攻击过程的行为模式(黑客行为模式)。二是对常见的黑客攻击方式，如缓冲区溢出攻击、口令穷举攻击等，提取出有状态攻击特征，作为黑客攻击特征库中的基本攻击特征。三是不断分析已经发现的黑客攻击行为，提取出攻击特征，及时添加到黑客攻击特征库中。四是针对常用操作系统和应用程序新发现的漏洞，设计黑客可能的攻击行为，在黑客攻击特征库中增加用于描述这些攻击行为的攻击特征。五是在通往重要服务器的链路上设置携带黑客行为模式和黑客攻击特征库的网络入侵检测系统。在重要服务器上设置携带用于检测进出主机信息的攻击特征库的主机入侵检测系统，针对已发现的主机所用操作系统和应用程序漏洞，对主机入侵检测系统设置防止黑客利用漏洞上传并激活蠕虫、篡改和删除重要系统文件的资源访问控制列表。

12.1.2　设计题解析

【例题 12.6】 互连网结构如图 12.1 所示，傀儡终端是已经被黑客控制的终端，黑客可以通过傀儡终端发起分布式拒绝服务攻击。为了检测分布式拒绝服务攻击，需要在互连网中设置网络入侵检测系统，给出设置网络入侵检测系统的位置，并简述网络入侵检测系统防御分布式拒绝服务攻击的原理。

【解析】

(1) 设置网络入侵检测系统的位置如图 12.2 所示，在这个位置设置网络入侵检测系统的目的是检测傀儡主机对网络 4 和网络 5 发起的攻击。

(2) 为了应对傀儡主机实施的直接攻击，网络入侵检测系统需要设置目的 IP 地址相

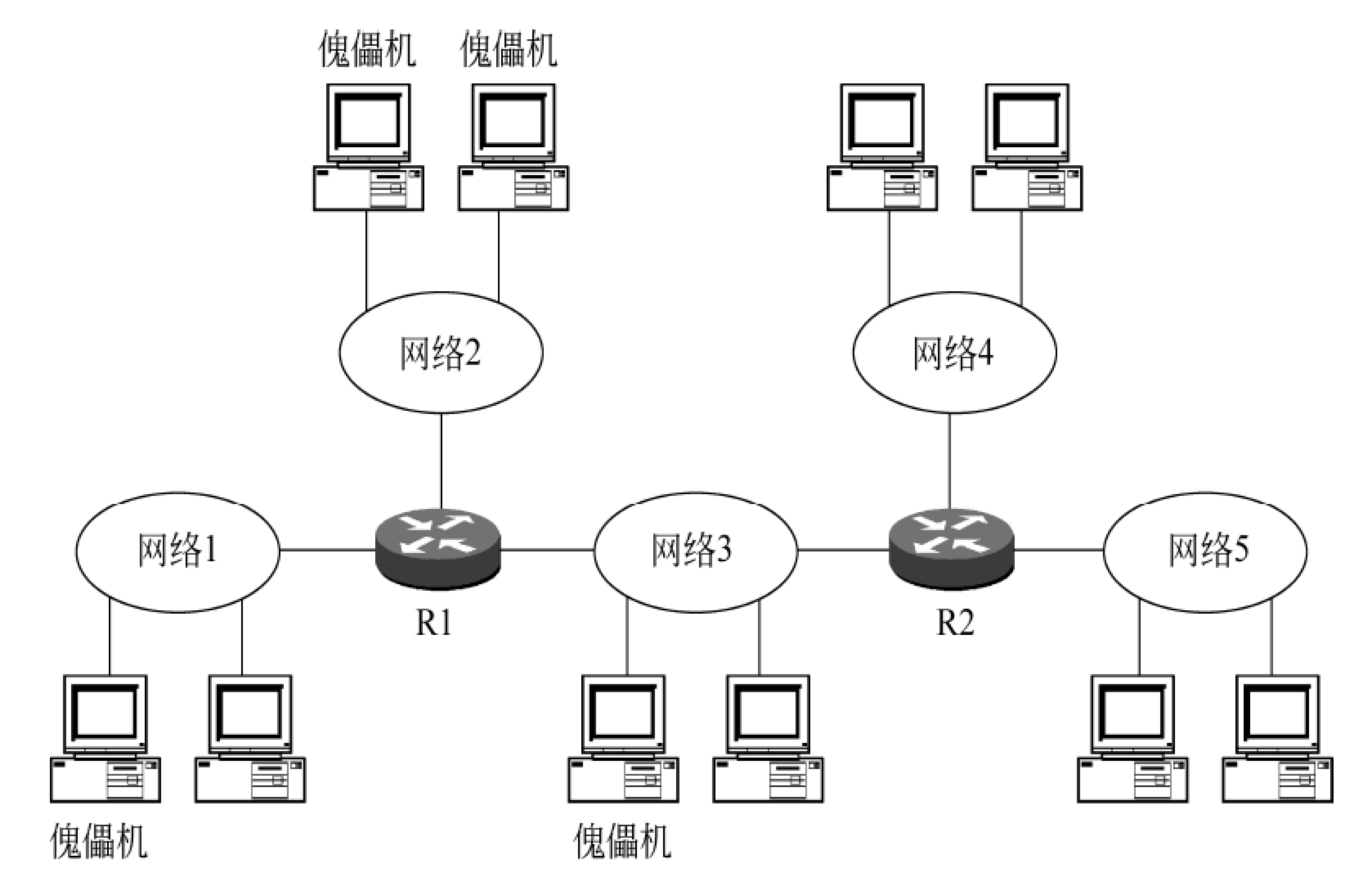


图 12.1 互连网结构

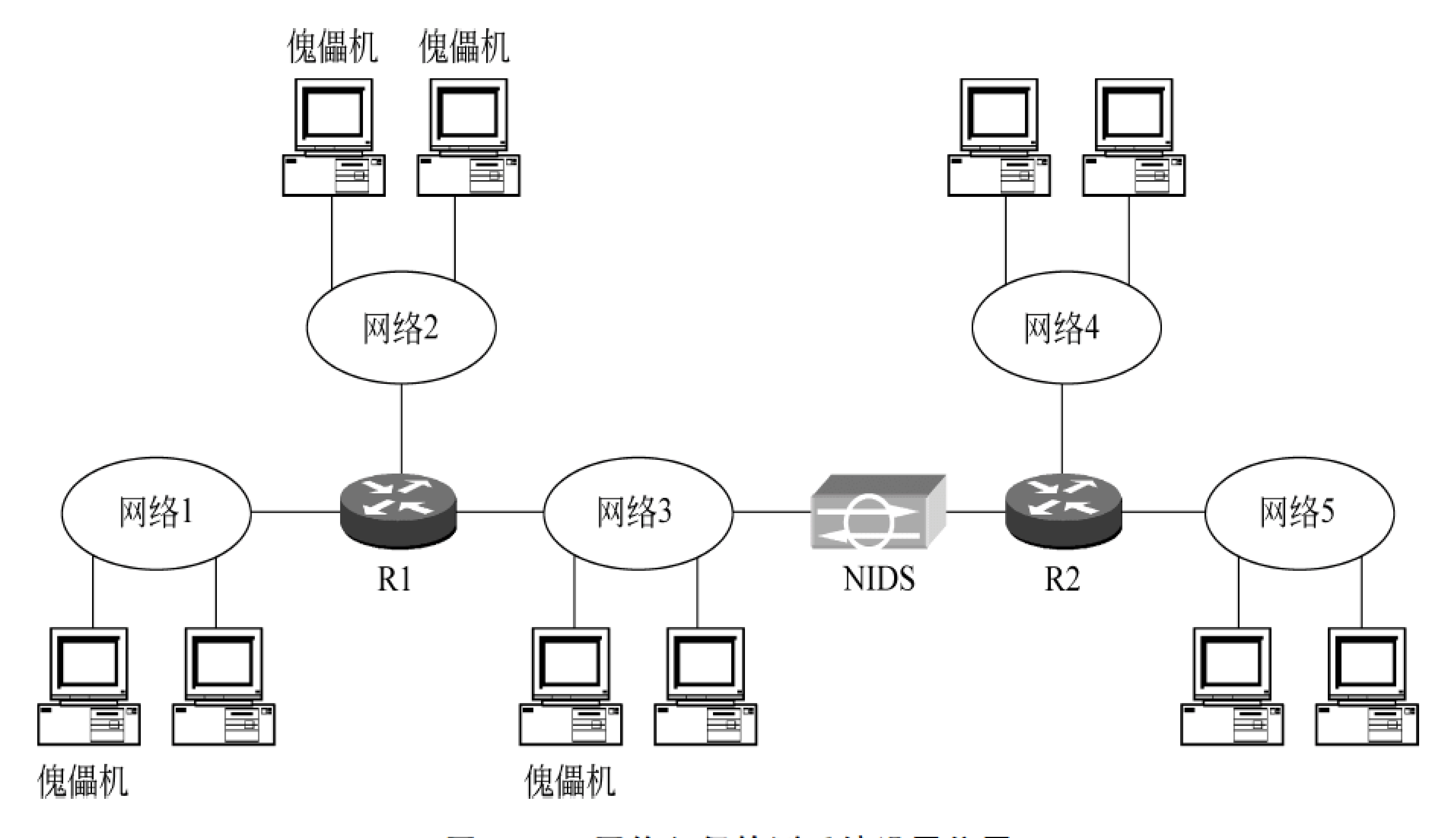


图 12.2 网络入侵检测系统设置位置

同、净荷是 UDP 报文或 ICMP ECHO 请求报文的 IP 分组阈值，一旦单位时间内接收到的目的 IP 地址相同、净荷是 UDP 报文或 ICMP ECHO 请求报文的 IP 分组数量超过阈值，则丢弃超过阈值部分的 IP 分组。

(3) 为了应对傀儡主机实施的间接攻击，网络入侵检测系统需要设置以下两个阈值：一是源 IP 地址相同、净荷是 ICMP ECHO 请求报文的 IP 分组阈值；二是目的 IP 地址相同，净荷是 ICMP ECHO 响应报文的 IP 分组阈值。一旦单位时间内接收到的源 IP 地址相同、净荷是 ICMP ECHO 请求报文的 IP 分组数量和目的 IP 地址相同、净荷是 ICMP ECHO 响应报文的 IP 分组数量超过阈值，则丢弃超过阈值部分的 IP 分组。

【例题 12.7】 假定网络结构如图 12.3 所示，要求：

(1) 能够检测感染蠕虫病毒的终端通过发送大量邮件传播病毒的过程；

(2) 能够检测对服务器发起的猜测登录口令攻击；

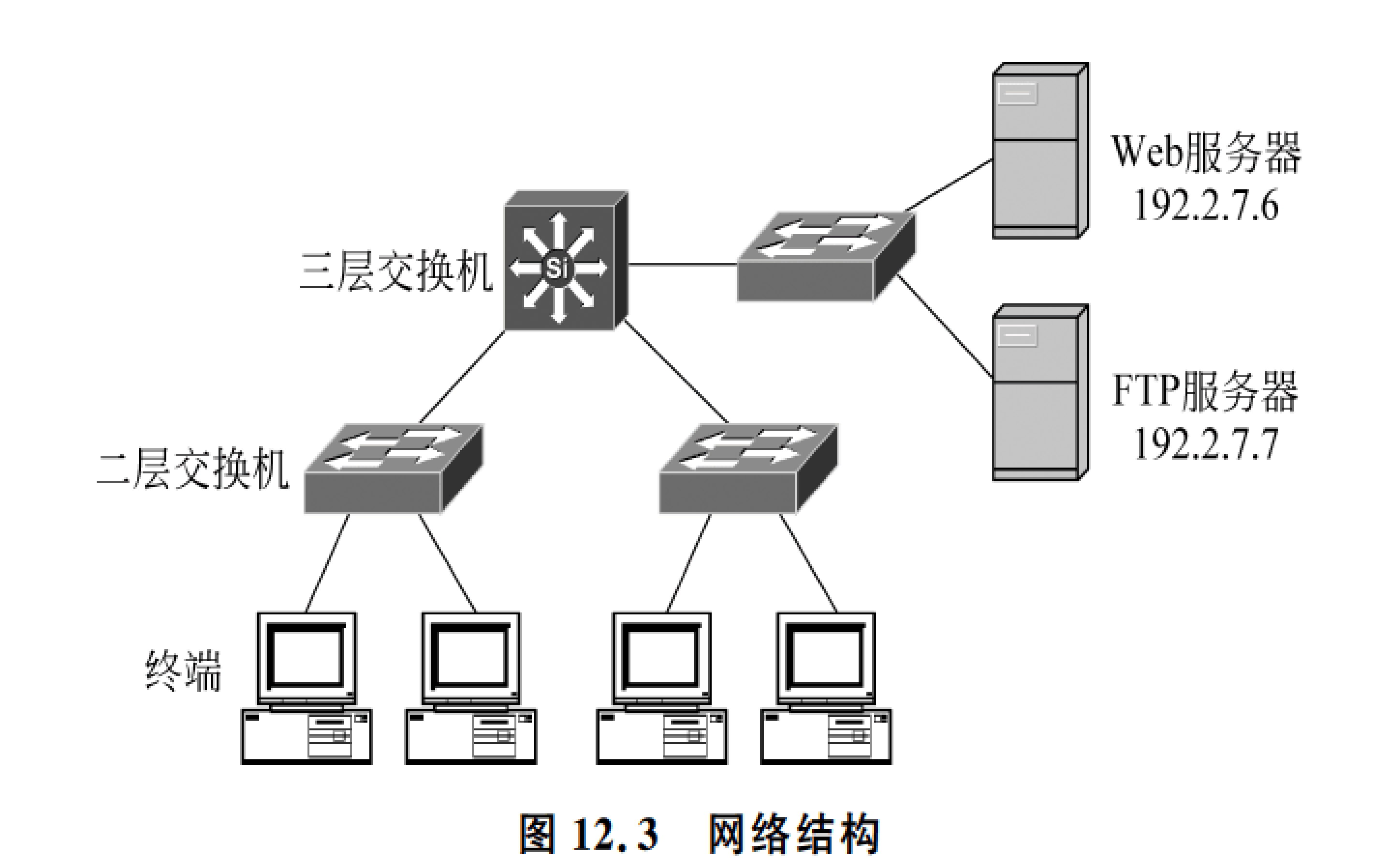


图 12.3　网络结构

(3) 能够检测黑客终端利用服务器木马病毒控制服务器的操作过程。

给出入侵检测系统的设置和配置信息,并简述实现上述要求的机制。

【解析】

(1) 网络入侵检测系统设置位置如图 12.4 所示。这样设置网络入侵检测系统的目的有两个:一是可以检测所有终端与服务器之间传输的信息;二是可以检测所有位于不同网络的终端之间传输的信息。

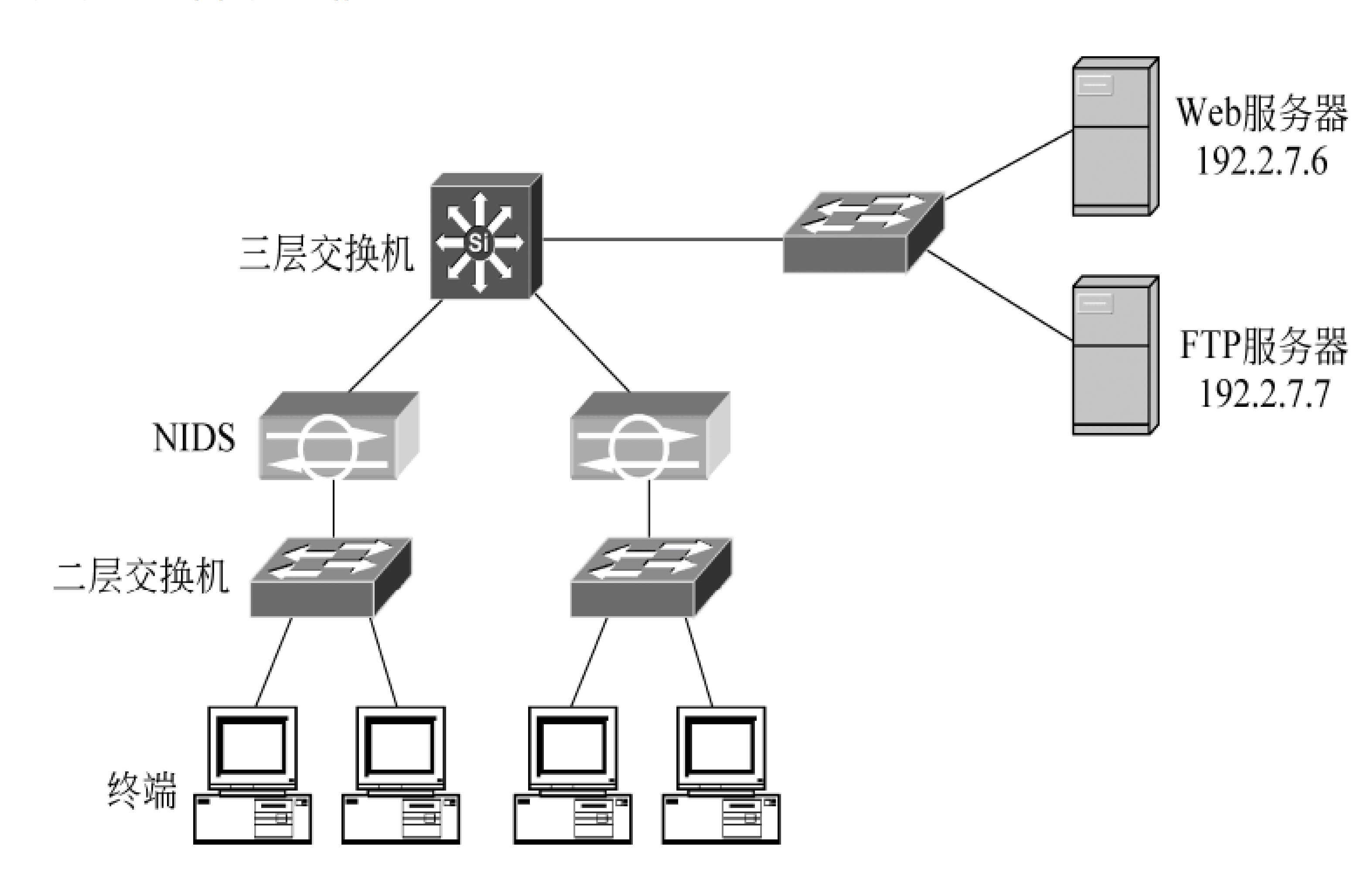


图 12.4　网络入侵检测系统设置位置

(2) 网络入侵检测系统配置的安全策略如表 12.1 所示,对服务器发起的猜测登录口令攻击过程和利用服务器木马病毒控制服务器的操作过程所涉及的信息传输过程符合交换式信息特征。感染蠕虫病毒的终端发送大量用于传播病毒的邮件的过程所涉及的信息传输过程符合邮件病毒特征。

表 12.1　安全策略

规则编号	源 IP 地址	目的 IP 地址	检测机制	攻击类型	动作
1	*	192.2.7.6/32	异常检测	交互式信息	源 IP 阻塞
2	*	192.2.7.7/32	异常检测	交互式信息	源 IP 阻塞
3	*	*	异常检测	邮件病毒	源 IP 阻塞

(3) 判断交换式信息的规则

① 相邻 TCP 报文的最小间隔大于 500ms。

② 相邻 TCP 报文的最大间隔小于 30s。

③ 背靠背 TCP 报文的比例大于 50%。

④ TCP 小报文(TCP 报文包含的字节数大于 20B 且小于 100B)的比例大于 80%。

(4) 判断邮件病毒的规则

① 终端的平均传输速率大于 6Mb/s。

② 超过 100ms 连续成组传输 IP 分组(成组传输是指相邻 IP 分组的时间间隔小于 5μs 的情况)的概率大于 7%。

③ 电子邮件在所有发送的信息中所占的比例大于 20%。

【例题 12.8】 如果图 12.3 中的 FTP 服务器中的内容极其敏感,需要严格限制授权终端下载 FTP 服务器中文件的操作,绝不允许删除或修改 FTP 服务器中的文件,如何通过设置和配置入侵检测系统做到这一点?

【解析】

(1) 网络入侵检测系统设置位置如图 12.5 所示。这样设置网络入侵检测系统的目的是使网络入侵检测系统只用于检测对 FTP 服务器实施的攻击。

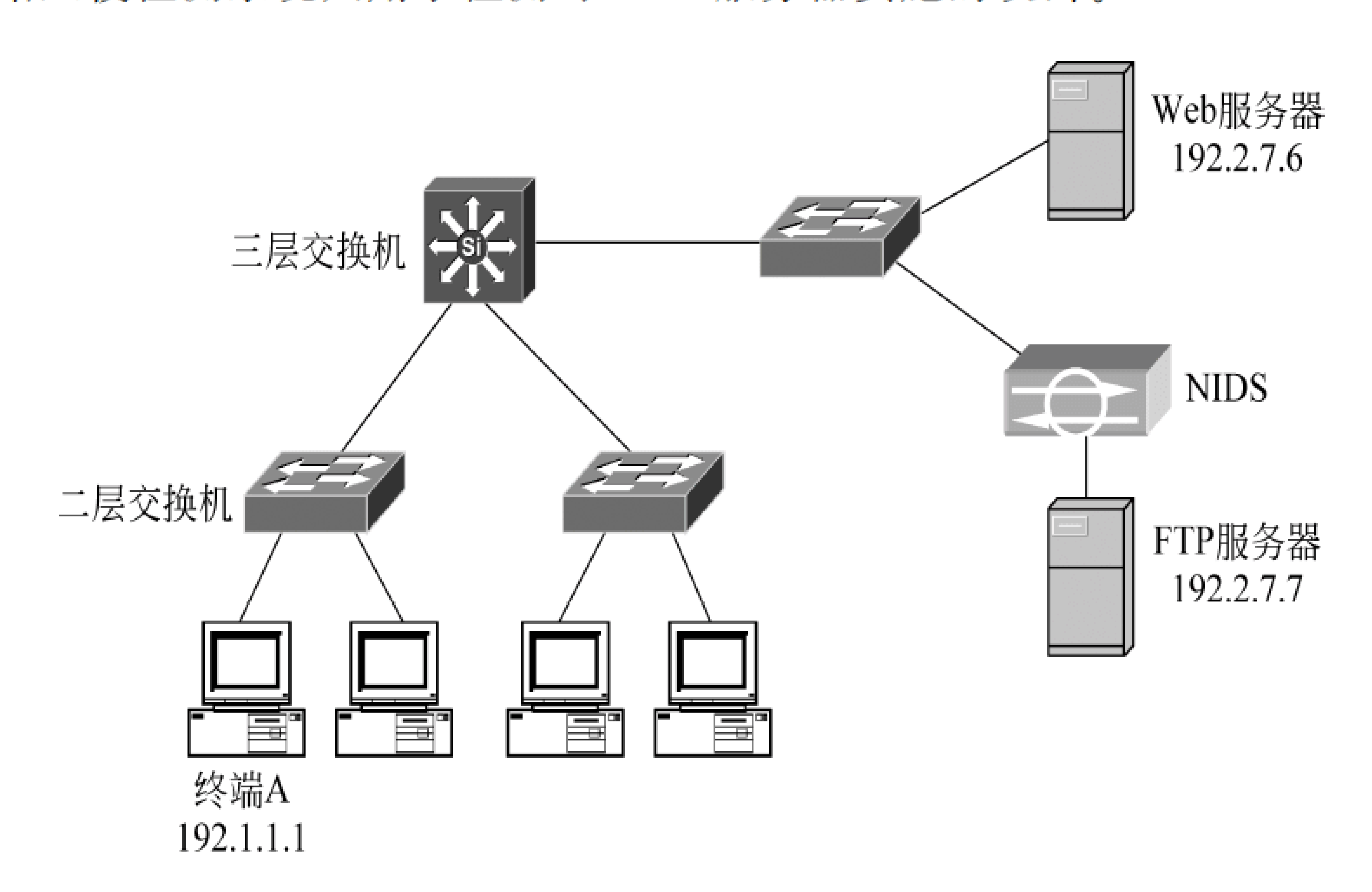


图 12.5 网络入侵检测系统设置位置

(2) 网络入侵检测系统配置的安全策略如表 12.2 所示,源 IP 地址范围严格限制了授权终端范围。服务 FTP GET 只允许与下载文件的操作过程有关的信息交换过程正常进行。加载已经发现的与攻击 FTP 服务器有关的所有攻击特征。

表 12.2 安全策略

规则编号	源 IP 地址	目的 IP 地址	服务	攻击特征库	动作
1	192.1.1.1/32	192.2.7.7/32	FTP GET	FTP—严重	源 IP 阻塞
				FTP—中等	源 IP 阻塞
				FTP—轻度	源 IP 阻塞

12.2　选择题分析

(1) 关于入侵,以下哪一项描述是错误的?(　　)

A. 破坏信息可用性的行为　　B. 破坏信息完整性的行为

C. 破坏信息保密性的行为　　D. 非法闯入

答案:D

【分析】 网络安全范畴中的入侵主要是指破坏网络中信息的可用性、完整性和保密性的行为,而不是指闯入没有授权进入的领地的行为。

(2) 关于入侵手段,以下哪一项描述是错误的?(　　)

A. 恶意代码　　B. 非法访问

C. 拒绝服务攻击　　D. 黑客

答案:D

【分析】 黑客是入侵者的称呼,不是入侵手段。

(3) 以下哪一项不是产生入侵检测系统的原因?(　　)

A. 与攻击有关的信息流无处不在

B. 攻击行为与正常访问过程存在差别

C. 杀毒软件不具有发现非法资源访问操作的功能

D. 控制网络间数据交换过程

答案:D

【分析】 这是防火墙已经实现的功能。

(4) 关于入侵检测系统,以下哪一项描述是错误的?(　　)

A. 一般的入侵检测系统和杀毒软件一样,需要定时更新攻击特征库

B. 正常访问过程和入侵过程存在差异,但无法严格区分

C. 规则是长期观察信息流变化过程后得出的一些规律性的总结

D. 入侵检测系统能够检测出没有发作的病毒

答案:D

【分析】 入侵检测系统主要检测发生在主机和网络中的异常行为,病毒不发作时,并不发生异常行为。

(5) 以下哪一项关于入侵检测系统功能的描述是错误的?(　　)

A. 防御病毒发作引发的攻击行为　　B. 防御对资源的非法访问

C. 防御分布式拒绝服务攻击　　D. 防御信息嗅探和截获攻击

答案:D

【分析】 这不是入侵检测系统能够防御的,需要通过精心设计网络拓扑结构和增强网络转发设备(路由器和交换机)的安全功能实现防御。

(6) 以下哪一项是入侵检测系统能够防御的攻击行为?(　　)

A. 路由项欺骗攻击　　B. 重放攻击

C. DNS 欺骗攻击　　D. 源 IP 地址欺骗攻击

答案：D

【分析】 有些源 IP 地址欺骗攻击采用固定格式的源 IP 地址，攻击特征检测机制能够检测出此类源 IP 地址欺骗攻击。

(7) 关于入侵检测系统功能，以下哪一项描述是错误的？(　　)

A. 捕获流经关键链路的信息流　　B. 发现攻击行为

C. 反制攻击行为　　D. 预防攻击行为

答案：D

【分析】 入侵检测系统的基本功能是检测出正在实施的攻击行为，并予以反制，并不能预先阻止攻击行为的发生。

(8) 以下哪一项不是入侵检测系统通用框架中的构件？(　　)

A. 事件发生器　　B. 事件分析器

C. 事件数据库　　D. 事件捕获器

答案：D

【分析】 入侵检测系统通用框架中没有事情捕获器，事情发生器的作用是提供需要检测的信息。

(9) 关于在线方式，以下哪一项描述是错误的？(　　)

A. 流经关键链路的信息必须经过入侵检测系统

B. 实时阻断入侵信息的传输过程

C. 要求较强的处理能力

D. 有着多种捕获信息的方式

答案：D

【分析】 在线方式下，流经关键链路的信息必须经过入侵检测系统，因此，不存在捕获信息的问题。

(10) 关于杂凑方式，以下哪一项描述是错误的？(　　)

A. 不影响信息流在关键链路的传输过程

B. 无法实时阻断入侵信息的传输过程

C. 有着多种捕获信息的方式

D. 要求较强的处理能力

答案：D

【分析】 杂凑方式对实时性要求不高，因此，对处理能力的要求低于在线方式。

(11) 关于主机入侵检测系统，以下哪一项描述是错误的？(　　)

A. 利用攻击特征库发现攻击行为

B. 根据访问授权发现非法资源访问过程

C. 禁止非法 TCP 连接建立

D. 保证主机不感染病毒

答案：D

【分析】 检测某个文件是否包含病毒不是入侵检测系统的主要功能，入侵检测系统主要检测病毒发作时发生的异常行为。

(12) 关于主机入侵检测系统的功能,以下哪一项描述是错误的?(　　)

A. 有效抵御恶意代码攻击　　B. 有效管制主机信息传输过程

C. 强化对主机资源的保护　　D. 有效抵御拒绝服务攻击

答案:D

【分析】 对于通过耗尽主机连接网络的链路的带宽,使主机无法和其他主机通信的拒绝服务攻击,主机入侵检测系统是无能为力的。

(13) 关于异常信息,以下哪一项描述是错误的?(　　)

A. 包含恶意代码的信息

B. 信息内容和指定应用不符的信息

C. 包含攻击特征的信息

D. 分组过滤器丢弃的信息

答案:D

【分析】 分组过滤器用于控制网络间通信过程,被分组过滤器丢弃的信息只是访问控制策略不允许正常传输的信息,未必是异常信息。

(14) 以下哪一项是入侵检测系统和防火墙相同的功能?(　　)

A. 利用攻击特征库发现攻击行为　　B. 作用于流经任何网段的信息

C. 阻断正常信息传输过程　　D. 阻断非法信息传输过程

答案:D

【分析】 防火墙阻断访问控制策略不允许传输的信息,入侵检测系统阻断违反安全策略或实施攻击的信息。

(15) 以下哪一项不是网络入侵检测系统的反制动作?(　　)

A. 丢弃 IP 分组　　B. 释放 TCP 连接

C. 报警和登记　　D. 隔离攻击源

答案:D

【分析】 在分布式拒绝服务攻击(DDoS)方式下,确定攻击源是一件非常困难的事情,因此,在检测到网络中存在攻击行为的情况下,网络入侵检测系统也很难确定并隔离攻击源。

(16) 以下哪一项不是主机入侵检测系统的反制动作?(　　)

A. 终止应用进程　　B. 拒绝操作请求

C. 释放 TCP 连接　　D. 全盘扫描

答案:D

【分析】 全盘扫描是杀毒软件的功能,主机入侵检测系统一般不会携带病毒特征库,并在检测到非法操作请求时启动全盘扫描过程。

(17) 关于理想的入侵检测系统,以下哪一项描述是错误的?(　　)

A. 没有误报　　B. 没有漏报

C. 具有线速检测信息流的能力　　D. 有着多种捕获信息的方式

答案:D

【分析】 杂凑方式下要求的多种捕获信息的方式,是由这种应用方式下的网络环境

提供的,不是由入侵检测系统独立实现的。

(18) 以下哪一项不是杂凑方式下捕获信息的方式?(　　)

A. 集线器　　B. 交换机端口镜像

C. 虚拟策略路由　　D. 路由协议

答案:D

【分析】 杂凑方式下捕获信息的方式要求同时做到以下两点:一是实现正常的信息传输过程,二是能够将信息转发给入侵检测系统。路由协议建立的传输路径可以实现正常的信息传输过程,但无法将信息转发给入侵检测系统。

(19) 以下哪一项是杂凑方式的探测器最有可能连接的设备?(　　)

A. 路由器　　B. 防火墙

C. 网关设备　　D. 交换机

答案:D

【分析】 探测器需要捕获信息,连接到交换机上可以通过端口镜像等方法捕获信息。

(20) 关于入侵检测机制,以下哪一项描述是错误的?(　　)

A. 检测某些字段取值是否超出正常范围

B. 检测流量分布是否和正常访问过程相似

C. 检测信息中是否包含攻击特征

D. 检测信息传输过程中是否被篡改

答案:D

【分析】 这是目的终端的完整性检测功能,不属于入侵检测机制的检测范围。

(21) 以下哪一项不是网络入侵检测系统的检测机制?(　　)

A. 攻击特征检测　　B. 协议译码

C. 异常检测　　D. 源端鉴别

答案:D

【分析】 网络入侵检测系统一般不会事先获知将要实施攻击的黑客终端,从而通过源端鉴别发现这些黑客终端发送的信息。

(22) 以下哪一项描述是错误的?(　　)

A. 单个 IP 分组可以包含全部元攻击特征

B. 元攻击特征可能分散在因为分片产生的多个 IP 分组中

C. 有状态攻击特征(组合攻击特征)需要记录状态迁移路径

D. 有状态攻击特征只能分布在属于同一 TCP 连接的多个 TCP 报文中

答案:D

【分析】 有状态攻击特征将攻击过程划分为多个不同阶段,每一个阶段包含对应的攻击特征,但没有要求这些阶段必须是同一 TCP 连接的不同阶段。

(23) 关于元攻击特征,以下哪一种描述是正确的?(　　)

A. 用于确定攻击信息的单个攻击特征

B. 一切攻击特征中不变的核心的字符串模式

C. 用于发现所有攻击的攻击特征

D. 攻击特征的最小单位

答案：A

【分析】 元攻击特征是指用于标识某个攻击的单一字符串。

(24) 关于有状态攻击特征,以下哪一项描述是错误的?(　　)

A. 用于确定攻击信息分散在信息流中的多个攻击特征

B. 这些攻击特征的出现位置和顺序都有严格的限制

C. 需要保存每一个阶段的检测状态

D. 多个攻击特征包含在属于同一 TCP 连接的 TCP 报文中

答案：D

【分析】 有状态攻击特征将攻击过程划分为多个不同的阶段,每一个阶段包含对应的攻击特征,但没有要求这些阶段必须是同一 TCP 连接的不同阶段。

(25) 以下哪一项描述是错误的?(　　)

A. 攻击特征检测机制容易漏报

B. 异常检测机制容易误报

C. 协议译码能够检测出恶意错误

D. 攻击特征检测机制能够检测出未知攻击

答案：D

【分析】 通过分析已经发现的攻击行为,才能提取出该攻击行为的特征信息。

(26) 对于采用攻击特征检测机制的网络入侵检测系统,以下哪一项是导致该网络入侵检测系统失效的原因?(　　)

A. 端到端加密传输　　B. 源 IP 地址欺骗

C. NAT　　D. 策略路由

答案：A

【分析】 网络入侵检测系统一般位于需要检测的信息必须经过的位置,因此,很难通过策略路由绕过。攻击特征通常包含在 IP 分组净荷或者传输层报文净荷中,因此,端到端加密传输是无法检测出攻击特征的主要原因。

(27) 关于协议译码,以下哪一项描述是错误的?(　　)

A. 检测 IP 分组首部

B. 检测 TCP 报文首部

C. 检测通过服务指定的信息交换过程

D. 检测 ESP 报文中的密文净荷

答案：D

【分析】 网络入侵检测系统无法对密文进行检测。

(28) 关于异常检测,以下哪一项描述是错误的?(　　)

A. 入侵行为有别于正常行为

B. 基于对正常行为的统计建立基准信息

C. 人工设置基准信息

D. 精确区分入侵行为和正常行为

答案：D

【分析】 正常访问网络的行为和攻击网络的行为之间存在重叠，因此，很难精确区分入侵行为和正常行为，故而存在误报或漏报的情况。

(29) 关于入侵检测机制，以下哪一项描述是错误的？(　　)

A. 协议译码可以阻断非法信息交换过程

B. 攻击特征检测可以检测出已经发现的攻击行为

C. 异常检测可以检测出一些未知的攻击行为

D. 网络入侵检测系统必须同时具备三种检测机制

答案：D

【分析】 不同网络入侵检测系统的差别很大，功能简单的网络入侵检测系统可能只具备攻击特征检测这一检测机制和根据已经发现的攻击行为得出的攻击特征库。

(30) 以下哪一项不属于网络入侵检测系统安全策略需要指定的信息？(　　)

A. 需要检测的信息流　　B. 检测机制和检测内容

C. 对入侵信息的反制动作　　D. 网络入侵检测系统的设置位置

答案：D

【分析】 安全策略是根据网络入侵检测系统需要完成的安全功能设计的，只有在确定网络入侵检测系统的设置位置后才能确定网络入侵检测系统需要完成的安全功能。

(31) 以下哪一项不属于拦截操作请求的机制？(　　)

A. 修改操作系统内核　　B. 系统调用拦截

C. 网络信息流监测　　D. 系统日志

答案：D

【分析】 系统日志只是记录进程和用户对系统实施的操作的信息。

(32) 关于主机入侵检测系统，以下哪一项描述是错误的？(　　)

A. 适合端到端加密传输情况

B. 可以检测出一些未知的攻击行为

C. 可以有效利用系统日志的信息

D. 可以发现主机扫描

答案：D

【分析】 主机扫描是指黑客对一组 IP 地址逐个进行 ping 操作，因此，主机入侵检测系统是无法根据接收到的单个 ICMP ECHO 请求报文判断出黑客是否正在进行主机扫描的。

(33) 以下哪一项不属于主机入侵检测系统安全策略需要指定的信息？(　　)

A. 操作请求发起者　　B. 操作

C. 对象　　D. 主机连接的网络类型

答案：D

【分析】 一般情况下，主机位置会影响主机资源访问权限，但主机连接的网络类型通常不会影响主机资源访问权限。

12.3 名词解释

(1) 入侵检测系统

一种可以获取流经关键链路的信息，并能够对这些信息进行检测，发现包含在这些信息中与实施攻击有关的有害信息，并予以反制的设备。

(2) 入侵

所有破坏网络中信息可用性、保密性和完整性的行为。

(3) 主机入侵检测系统

一种发现针对主机系统的入侵行为并予以反制的设备。

(4) 网络入侵检测系统

一种发现针对网络的入侵行为并予以反制的设备。

(5) 在线方式

一种网络入侵检测系统的应用方式，这种应用方式下，IDS 位于关键链路的中间，所有经过该关键链路传输的信息必须经过 IDS。

(6) 杂凑方式

一种网络入侵检测系统的应用方式，这种应用方式下，入侵检测系统对信息经过关键链路的传输过程没有影响，只能被动捕获经过关键链路传输的信息。因此，无法实时阻断入侵信息的传输过程。

(7) 攻击特征

用于鉴别是否是攻击信息的特定字符串模式。

(8) 元攻击特征

用于确定攻击信息的单个攻击特征。

(9) 有状态攻击特征

用于确定攻击信息的分散在信息流中的多个攻击特征。

(10) 协议译码

一种通过对 IP 分组格式、TCP 报文格式进行检测，根据 TCP 报文的目的端口字段值或 IP 报文的协议字段值确定报文净荷对应的应用层协议，然后根据协议要求对净荷格式、净荷中各字段内容、请求和响应过程进行检测，以此发现攻击信息的检测机制。

(11) 攻击特征检测

一种从已经发现的攻击中提取出能够标识这一攻击的特征信息，构成攻击特征库，然后对捕获到的信息进行攻击特征匹配操作，以此发现攻击信息的检测机制。

(12) 异常检测

一种需要事先建立正常网络访问过程下的信息流模式库和资源访问操作规则库，然后实时分析捕获到的信息，并根据捕获到的信息得出的信息流模式，或者根据捕获到的信息得出的网络资源访问操作与已经建立的信息流模式库或资源访问操作规则库中相应的信息流模式或访问操作规则之间是否存在较大偏差，发现攻击信息的检测机制。

(13) 误报

把正常的信息交换过程或网络资源访问过程作为攻击过程予以反制和报警的情况。

(14) 漏报

把攻击过程当作正常的信息交换过程或网络资源访问过程不予干预,从而使黑客攻击成功的情况。

第 13 章 病毒防御技术

13.1 例题解析

【例题 13.1】 简述阻止病毒传播和危害发生的措施。

【解析】 这些措施分为基于主机系统的措施和基于网络的措施，基于主机系统的措施有：及时运行补丁软件；安装查杀病毒软件；安装主机入侵检测系统；安装个人防火墙等。基于网络的措施有：在网络边界设置控制网络间信息交换过程的防火墙；在关键链路设置严格监控流经该段链路的信息流的网络入侵检测系统；采用隐藏内部网络的 NAT 技术；限制疑似与病毒传播和拒绝服务攻击有关的信息流的流量的流量管制技术等。

【例题 13.2】 内部网络综合病毒防御系统如图 13.1 所示，完成以下安全功能配置过程。

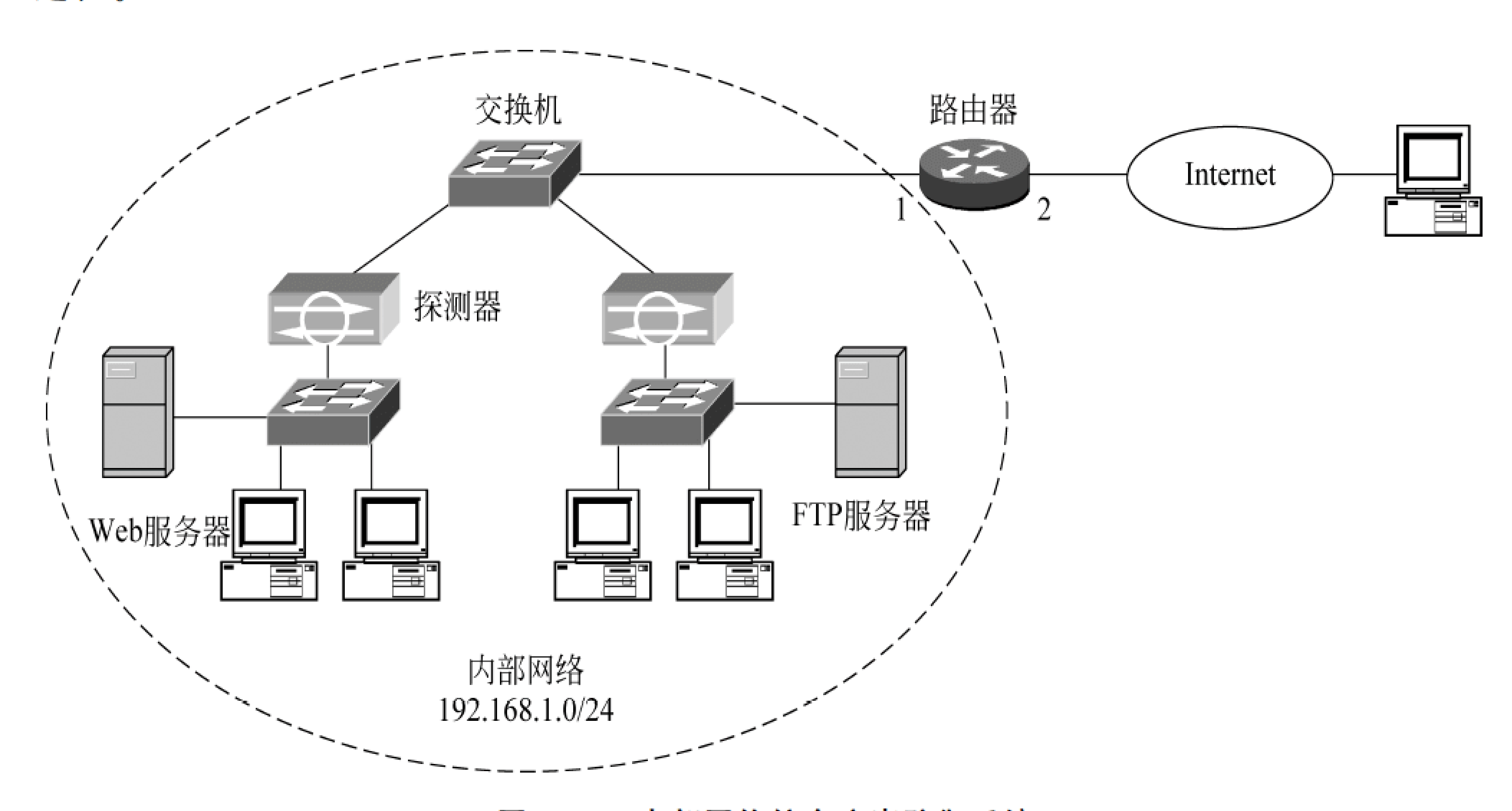


图 13.1 内部网络综合病毒防御系统

(1) 通过 NAT 隐藏内部网络。

(2) 通过设置有状态分组过滤器只允许与访问 Internet 中的 Web 服务器、FTP 服务器和 E-Mail 服务器的过程相关的 IP 分组输入/输出路由器接口 1。

(3) 通过设置入侵检测系统规则，要求能够有效阻止蠕虫病毒在内部网络的蔓延。

【解析】

(1) 路由器实现 PAT 功能，只允许由内部网络终端发起访问 Internet 的过程。内部

网络对于 Internet 是透明的。因此，Internet 中的黑客无法主动发起对内部网络终端的入侵过程。

(2) 路由器接口 1 输入方向设置如表 13.1 所示的分组过滤器，该分组过滤器只允许内部网络终端发送的与访问 Internet 中的 Web 服务器、FTP 服务器和 E-Mail 服务器的过程相关的 IP 分组输入路由器接口 1。路由器接口 1 输出方向设置如表 13.2 所示的分组过滤器，该分组过滤器禁止一切 IP 分组输出。

表 13.1 路由器接口 1 输入方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	TCP	192.168.1.0/24	*	>1023	80	允许
2	TCP	192.168.1.0/24	*	>1023	21	允许
3	TCP	192.168.1.0/24	*	>1023	20	允许
4	TCP	192.168.1.0/24	*	>1023	25	允许
5	TCP	192.168.1.0/24	*	>1023	110	允许
6	*	*	*	_	_	拒绝

表 13.2 路由器接口 1 输出方向分组过滤器

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1	*	*	*	_	_	拒绝

路由器接口 1 输入方向设置监测以下应用层协议的监测器。

HTTP

FTP

SMTP

POP3

一旦路由器接口 1 输入方向监测到上述应用层协议的请求消息，路由器接口 1 输出方向动态增加允许这些请求消息对应的响应消息输出的过滤器规则。以此保证路由器接口 1 只允许输入/输出与内部网络终端发起的、访问 Internet 中的 Web 服务器、FTP 服务器和 E-Mail 服务器的过程相关的 IP 分组。

(3) 为探测器设置用于阻止通过邮件传播病毒的规则。一旦检测到违反以下规则的信息流，则阻塞源终端一段时间 T。

阻止通过邮件传播病毒的规则如下。

① 每一个终端的平均传输速率小于等于 3Mb/s。

② 超过 100ms 连续成组传输 IP 分组(成组传输是指相邻 IP 分组的时间间隔小于 5μs 的情况)的概率小于等于 1%。

③ 电子邮件在所有发送的信息中所占的比例小于等于 10%。

为探测器设置用于发现蠕虫病毒传播过程的攻击特征。一旦检测到符合攻击特征的信息流，阻塞源终端一段时间 T。

用于发现蠕虫病毒传播过程的攻击特征如下。

- 单位时间内源 IP 地址相同、目的端口号为 80 的请求建立 TCP 连接的请求报文数量大于等于 500。
- 包含特定引导程序代码的 HTTP 请求消息。
- 建立反向连接。

13.2　选择题分析

(1) 以下哪一项病毒通常不是寄生病毒？(　　)

A. 脚本病毒　　B. 宏病毒

C. PE 病毒　　D. 蠕虫病毒

答案：D

【分析】 蠕虫病毒通常是一个独立、完整的程序。

(2) 以下哪一项不是常见的将病毒植入主机的方式？(　　)

A. 移动媒体　　B. 访问网页

C. 邮件附件　　D. 运行正版软件

答案：D

【分析】 正规厂商发行的正版软件中不会嵌入病毒程序。

(3) 以下哪一项不是常见的第一次运行病毒的方式？(　　)

A. 插入包含 AutoRun 病毒的 U 盘

B. 浏览包含脚本病毒的网页

C. 打开包含宏病毒的 Office 文档

D. 接收到附件是包含病毒的可执行程序的邮件

答案：D

【分析】 只要不人工运行附件中包含病毒的可执行程序，计算机就不会自动启动附件中的病毒程序。

(4) 以下哪一项不是常见的计算机自动激发病毒的方式？(　　)

A. 将病毒嵌入 BIOS 和引导区

B. 将病毒程序作为自启动项

C. 将病毒嵌入常用设备的设备驱动程序

D. 为病毒程序创建桌面快捷方式

答案：D

【分析】 计算机不会自动启动桌面快捷方式对应的病毒程序。

(5) 关于病毒感染，以下哪一项描述是错误的？(　　)

A. 将宏病毒嵌入 Office 文档中

B. 将脚本病毒嵌入 HTML 文档中

C. 将 PE 病毒嵌入 PE 格式文件中

D. 将病毒程序嵌入信箱中邮件的附件中

答案：D

【分析】 信箱中的邮件一般都是已经发送或者接收的邮件，将病毒程序嵌入信箱中邮件的附件中，已经没有意义。不过，在病毒发作时，可能会生成大量附件是病毒程序的邮件，并将这些邮件发送给信箱。

(6) 以下哪一项不是病毒可能实施的破坏活动？(　　)

A. 破坏硬盘中的信息　　B. 发起拒绝服务攻击

C. 破坏 BIOS 中的信息　　D. 损坏主板器件

答案：D

【分析】 由于 BIOS 支持在线擦除和写入，因此，病毒可以破坏 BIOS 中的信息，但病毒一般不能破坏主板上的其他器件。

(7) 关于基于主机的病毒防御技术，以下哪一项描述是错误的？(　　)

A. 通过检测程序中的病毒代码特征确定程序是否包含病毒

B. 通过分析程序中的功能模块确定程序是否包含病毒

C. 通过监控程序的行为确定该程序是否是病毒程序

D. 通过追踪程序的生成者确定该程序是否是病毒程序

答案：D

【分析】 对于具有数字签名的程序，确定程序的生成者是比较方便的，对于用户编写的一般应用程序，确定程序的生成者是比较困难的。因此，基于主机的病毒防御技术不会简单地根据能否确定程序生成者确定该程序是否是病毒程序。

(8) 以下哪一项病毒的变种处理对避免病毒被基于特征的扫描技术发现是无效的？(　　)

A. 压缩病毒　　B. 用随机产生的密钥加密病毒

C. 随机插入无效代码　　D. 指令同义替换

答案：A

【分析】 避免被基于特征的扫描技术发现的前提是每一次变形处理后的结果都是不同的。但同一段代码每一次压缩处理后的结果是相同的。

(9) 关于基于特征的扫描技术，以下哪一项描述是错误的？(　　)

A. 事先建立病毒特征库

B. 病毒特征是可以标识某个病毒的一段代码或文本内容

C. 病毒特征是通过分析已经发现的病毒提取的

D. 病毒特征可以标识未发现的病毒

答案：D

【分析】 病毒特征是通过分析已经发现的病毒提取的该病毒有别于正常代码或文本的特征信息，不能标识未知病毒。

(10) 关于基于线索的扫描技术，以下哪一项描述是错误的？(　　)

A. 不需要精确匹配病毒特征

B. 通过分析可执行文件入口处代码的功能确定该文件是否感染病毒

C. 可以发现变形病毒和未知病毒

D. 可以取代基于特征的扫描技术

答案：D

【分析】 基于线索的扫描技术只能作为基于特征的扫描技术的补充，用于发现一些变形和未知的病毒，不是主流的基于主机的病毒防御技术。

(11) 关于基于完整性检测的扫描技术，以下哪一项描述是错误的？(　　)

A. 不需要精确匹配病毒特征　　B. 可以发现变形病毒和未知病毒

C. 不需要分析文件中的代码功能　　D. 可以发现文件的任何改变

答案：D

【分析】 基于完整性检测的扫描技术通过检测一段时间内文件是否发生改变判断文件是否感染病毒。判断文件是否改变的依据是文件的报文摘要。没有一种报文摘要算法可以保证能够通过报文摘要检测出文件发生的任何改变。

(12) 以下哪一项病毒检测机制是检测系统软件是否感染病毒的有效方法？(　　)

A. 基于特征的扫描技术　　B. 基于线索的扫描技术

C. 基于完整性检测的扫描技术　　D. 基于行为的检测技术

答案：C

【分析】 在较长时间内不变的系统软件适合采用基于完整性检测的扫描技术，用该扫描技术可以发现被大多数已知和未知病毒感染的文件。

(13) 关于基于行为的检测技术，以下哪一项描述是错误的？(　　)

A. 需要为不同用户配置访问权限

B. 需要监控用户进程发出的操作请求

C. 可以发现变形病毒和未知病毒

D. 可以用访问权限精确区分病毒行为和正常访问操作

答案：D

【分析】 基于行为的检测技术由于很难区分正常和非正常的资源访问操作，因而无法为用户精确配置资源访问权限，所以常常发生漏报和误报病毒的情况。

(14) 关于基于模拟运行环境的检测技术，以下哪一项描述是错误的？(　　)

A. 事先建立已知病毒的操作特征库和资源访问原则

B. 在软件仿真环境中模拟程序的执行过程

C. 可以监控病毒程序的破坏结果

D. 可以作为一种独立使用的病毒检测技术

答案：D

【分析】 该病毒检测技术需要与其他基于主机的病毒检测技术一起使用，一般情况下，由其他病毒检测技术发现疑似病毒程序，然后由基于模拟运行环境的检测技术确定是否是病毒程序。

(15) 以下哪一项描述是错误的？(　　)

A. 安装杀毒软件的机器是安全的

B. 防火墙具有阻止病毒传播的功能

C. 入侵检测系统具有发现病毒的功能

D. 操作系统漏洞是机器感染病毒的主要原因

答案：A

【分析】 一般情况下，杀毒软件只能查杀病毒特征已经包含在病毒特征库中的已知病毒。

(16) 防火墙能有效阻止以下哪一项病毒传播方式？(　　)

A. 利用主机系统漏洞自动传播病毒　　B. 通过邮件传播病毒

C. 通过 Web 页面传播病毒　　D. 通过实用程序传播病毒

答案：A

【分析】 防火墙只能通过访问控制策略禁止一些信息交换过程，其他三种传播方式往往利用访问控制策略允许进行的信息交换过程传播病毒。

(17) 关于防火墙，以下哪一项描述是错误的？(　　)

A. 防火墙主要用于控制网络之间的数据交换过程

B. 防火墙能有效抑制内网终端中的木马外泄信息

C. 防火墙能减缓拒绝服务攻击

D. 防火墙能杜绝病毒从一个网络传播到另一个网络

答案：D

【分析】 防火墙的主要功能是控制网络间数据的交换过程，检测数据中是否携带病毒不是防火墙的主要任务，杜绝病毒传播更是不可能的。

(18) 网络入侵检测系统对以下哪一项病毒传播方式不起作用？(　　)

A. 利用主机系统漏洞自动传播病毒　　B. 通过邮件传播病毒

C. 通过 Web 页面传播病毒　　D. 通过实用程序传播病毒

答案：D

【分析】 通过攻击特征匹配和访问控制策略能发现 A 选项的传播方式。通过精心设置阈值和规则也能发现 B 选项的传播方式。通过深入检查、分析一段时间内相互交换的信息可以发现 C 选项的传播方式。除非实用程序包含已经提取出病毒特征的病毒，且网络入侵检测系统具有根据病毒特征库查杀病毒的功能，否则，静态分析某个实用程序是否包含病毒是很难的。

13.3　名词解释

(1) 病毒

一种具有感染和传播能力的特殊的恶意代码。

(2) 寄生病毒

一段寄生在其他程序和文件中的恶意代码。

(3) 脚本病毒

一段用脚本语言编写的嵌入在 HTML 文档中的恶意代码。

(4) 宏病毒

一段由 VBA 编写的以宏的形式寄生在 Office 文档中的恶意代码。

(5) PE 病毒

一段嵌入在 PE 格式文件中的恶意代码。

(6) AutoRun 病毒

一种通过修改 U 盘的 AutoRun.inf 文件和启动 Windows 系统的自动播放功能,使计算机能够在打开 U 盘时自动执行的病毒程序。

(7) 蠕虫病毒

一种能够自动完成植入和运行过程的非寄生病毒程序。

(8) 木马病毒

一种旨在削弱主机系统的安全机制,为黑客访问主机系统资源提供方便的病毒程序。

(9) 基于特征的扫描技术

一种通过分析已经发现的病毒,提取出每一种病毒有别于正常代码或文本的病毒特征,并以此建立病毒特征库。然后根据病毒特征库在扫描的文件中进行匹配操作,以此确定该文件是否包含病毒的病毒检测技术。

(10) 基于线索的扫描技术

一种通过分析可执行文件入口处代码的功能确定该文件是否感染病毒的病毒检测技术。

(11) 基于完整性检测的扫描技术

一种通过定期检测文件是否发生改变确定该文件是否包含病毒的病毒检测技术。

(12) 基于行为的检测技术

一种根据程序运行过程中的行为判断该程序是否是病毒程序的病毒检测技术。

(13) 基于模拟运行环境的检测技术

一种通过在软件仿真环境中模拟程序的执行过程,并根据程序执行过程中产生的一系列操作判断该程序是否是病毒程序的病毒检测技术。

第 14 章

计算机安全技术

14.1 例题解析

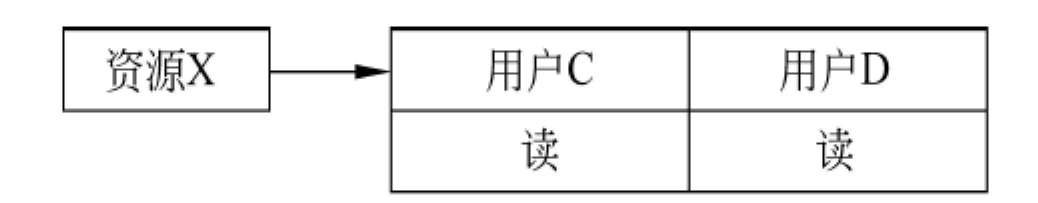
【例题 14.1】 如果访问控制矩阵如表 14.1 所示，给出对应的访问控制表和访问能力表。

表 14.1 访问控制矩阵

主体	客　体		
	资源 X	资源 Y	资源 Z
用户 A		读、修改、管理	读、修改、管理
用户 B		读、修改、管理	
用户 C	读	读、修改	
用户 D	读	读、修改	读、修改、管理

【解析】

(1) 访问控制表如图 14.1 所示。



(a) 资源X访问控制表

资源Y →

用户A	用户B	用户C	用户D
读、修改、管理	读、修改、管理	读、修改	读、修改

(b) 资源Y访问控制表



(c) 资源Z访问控制表

图 14.1 访问控制表

(2) 访问能力表如图 14.2 所示。

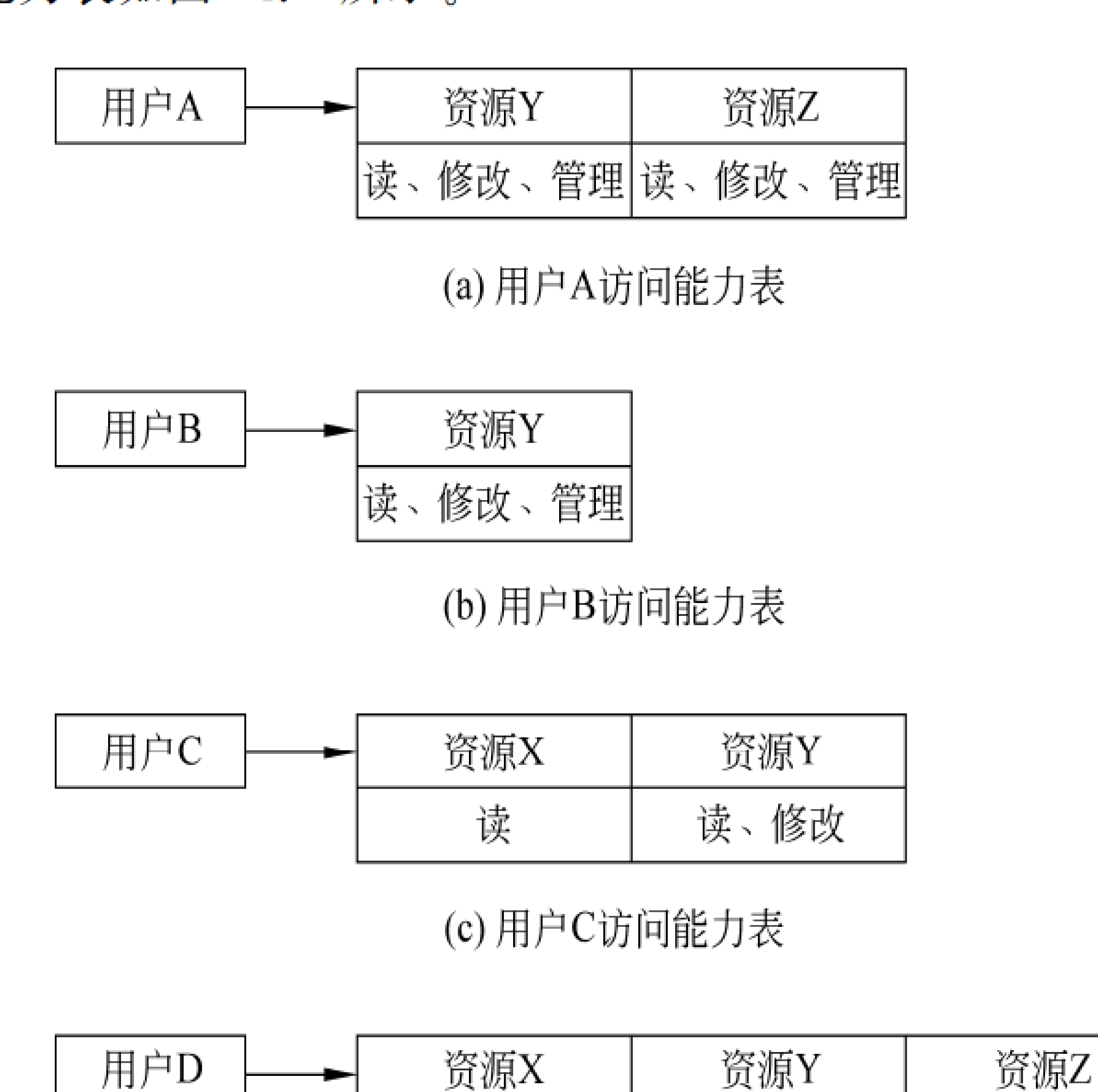


图 14.2 访问能力表

14.2 选择题分析

(1) 以下哪一项不是网络环境中主机的安全威胁?(　　)

A. 病毒　　B. 黑客入侵

C. 越权访问　　D. 密码策略

答案: D

【分析】 密码策略可以保证用户配置安全的密码。

(2) 以下哪一项不属于计算机安全技术?(　　)

A. 病毒防御技术　　B. 个人防火墙

C. 主机入侵检测系统　　D. VPN

答案: D

【分析】 VPN 主要用于实现跨互连网安全传输数据的过程,不能算是计算机安全技术。

(3) 以下哪一项是为了防范计算机系统和资源被未授权访问而采取的第一道防线?(　　)

A. 访问控制　　B. 授权　　C. 审计　　D. 加密

答案: A

【分析】 访问控制的主要功能之一就是拒绝非授权用户非法获取资源。授权和审计是访问控制的组成部分。加密是一种在访问控制失败后,用于保证资源保密性的技术。

(4) 以下哪一项与访问控制实现过程无关?(　　)

A. 身份鉴别　　B. 授权

C. 访问控制　　D. 客体加密

答案:D

【分析】 访问控制是保证主体只能访问授权访问的客体,且只能对客体进行授权的操作。因此,客体加密只有在访问控制失败的情况下才有用。

(5) 以下哪一项不是访问控制模型的缩写?(　　)

A. DAC　　B. MAC　　C. RBAC　　D. TCSEC

答案:D

【分析】 TCSEC 是可信计算机评估准则的英文缩写。

(6) 关于自主访问控制模型,以下哪一项描述是错误的?(　　)

A. 基于主体或主体所属的主体组的身份限制主体对客体的访问

B. 自主是指拥有资源的主体能够自主地将访问权限或访问权限的某个子集授予其他主体

C. 用访问控制矩阵表示一组主体对一组客体的访问权限

D. 访问控制矩阵是描述访问控制策略的最佳方式

答案:D

【分析】 如果存在 m 个主体和 n 个客体,访问控制矩阵有着 $m\times n$ 个单元格。由于每一个主体只能授权访问有限个客体,因此,在每一行对应的 n 个单元格中,大量单元格是空白的。

(7) 关于访问控制表,以下哪一项描述是错误的?(　　)

A. 以客体为中心,为每一个客体分配访问权限

B. 访问控制表是操作系统最常用的访问控制模型

C. 访问控制表中列出所有允许访问该客体的主体和主体对该客体的访问权限

D. 访问控制表一般用于对客体分布式管理的应用环境

答案:D

【分析】 访问控制表一般用于对客体集中管理的应用环境。用户登录主机后,可以对集中在该主机中且允许该用户访问的所有客体进行访问。

(8) 关于访问能力表,以下哪一项描述是错误的?(　　)

A. 以主体为中心,为每一个主体分配访问权限

B. 访问能力表中列出所有允许该主体访问的客体和该主体对客体的访问权限

C. 访问能力表一般用于对客体分布式管理的应用环境

D. 访问能力表是操作系统最常用的访问控制模型

答案:D

【分析】 操作系统的功能之一是实现对主机中资源的访问控制过程,是一种对客体集中管理的应用环境,通常使用访问控制表。

(9) 关于自主访问控制,以下哪一项描述是错误的?(　　)

A. 由于分布式系统中很难确定给定客体的潜在主体集,访问能力表在分布式系

统中得到广泛应用

B. 基于矩阵中列的访问控制信息表示访问能力表，即每个客体附加一个它可以访问的主体的明细表

C. 自主访问控制模型的实现机制是通过访问控制矩阵实施的，而具体的实现办法则是通过访问能力表或访问控制表限定哪些主体针对哪些客体可以执行什么操作

D. 系统中的访问控制矩阵本身通常不被完整地存储，因为矩阵中的许多元素常常为空

答案：B

【分析】 基于矩阵中列的访问控制信息表示访问控制表。

(10) 关于强制访问控制模型，以下哪一项描述是错误的？(　　)

A. 是系统强制主体服从的访问控制策略

B. 强制指对所有主体及所控制的客体实施强制访问控制

C. 每一个主体和客体赋予一个安全级别

D. 每一个主体只允许访问安全级别低于自己的客体

答案：D

【分析】 不同的安全要求有着不同的访问控制模型，如为了保证数据的保密性，要求不向下写，即只有当主体安全级别低于或等于客体安全级别时，才允许主体对客体进行写操作。

(11) 关于强制访问控制，以下哪一项描述是错误的？(　　)

A. Bell-LaPadula 模型具有只允许向下读、向上写的特点，可以有效地防止机密信息向下级泄露

B. Biba 模型具有不允许向下读、向上写的特点，可以有效地保护数据的完整性

C. 强制访问控制通过为每一个主体和客体赋予一个安全级别，实现了信息的单向流通

D. Biba 模型作为 BLP 模型的补充而提出，利用“不上读/不下写”的原则保证数据的完整性

答案：D

【分析】 Bell-LaPadula 和 Biba 是两种功能不同的强制访问控制模型，Bell-LaPadula 用于保证数据的保密性，而 Biba 用于保证数据的完整性，Biba 模型不是作为 BLP 模型的补充而提出的。

(12) 关于 Bell-LaPadula 模型，以下哪一项描述是错误的？(　　)

A. Bell-LaPadula 模型用于保证数据保密性

B. 要求主体不能对安全级别高于自己的客体进行读操作

C. Bell-LaPadula 模型的访问原则是不上读/不下写

D. 允许数据从安全级别高的客体流向安全级别低的客体

答案：D

【分析】 如果允许数据从安全级别高的客体流向安全级别低的客体,即使做到不上读,依然使主体能够读到安全级别高于自己的客体。

(13) 关于 Biba 模型,以下哪一项描述是错误的?(　　)

A. Biba 模型用于保证数据的完整性

B. 要求主体不能对安全级别高于自己的客体进行写操作

C. Biba 模型的访问原则是不下读/不上写

D. 允许数据从安全级别低的客体流向安全级别高的客体

答案:D

【分析】 数据完整性要求主体不能对安全级别高于自己的客体进行写操作。同时不允许数据从安全级别低的客体流向安全级别高的客体。

(14) 关于基于角色的访问控制模型,以下哪一项描述是错误的?(　　)

A. 基于角色分配权限

B. 每一个用户可以分配给多个角色

C. 每一个角色可以由多个用户构成

D. 通过身份鉴别过程确定用户角色

答案:D

【分析】 由于每一个用户可以分配给多个角色,因此,通常通过身份鉴别过程确定用户,而由用户自己选择角色。

(15) 以下哪一项不是审计系统的组成部分?(　　)

A. 日志记录器　　B. 分析器

C. 通告器　　D. 响应单元

答案:D

【分析】 一个审计系统通常由日志记录器、分析器和通告器三部分组成。这三部分分别用于收集数据、分析数据和通告结果。

(16) 关于 Windows 7 访问控制机制,以下哪一项描述是错误的?(　　)

A. 采用访问控制表(ACL)机制

B. 通过创建账户创建用户

C. 基于资源为每一个用户分配权限

D. 用户可以修改某个资源的访问权限

答案:D

【分析】 用户登录后,针对某个资源,只能根据分配给该用户的权限访问该资源。基于资源为每一个用户分配权限是系统管理员的功能。

(17) 关于 Windows 7 防火墙,以下哪一项描述是错误的?(　　)

A. 基于会话的有状态分组过滤器

B. 可以指定作为会话发起方或接收方的程序

C. 允许配置入站规则和出站规则

D. 会话指 TCP 连接

答案:D

【分析】 常见的会话有 TCP 连接、UDP 会话和 ICMP ECHO 请求、响应过程。

(18) 关于入站规则,以下哪一项描述是错误的?(　　)

A. 可以用 IP 地址唯一指定会话发起方所在的终端

B. 可以用端口号唯一指定作为会话发起方的进程

C. 可以用程序唯一指定作为会话响应方的进程

D. 入站规则用于禁止或允许创建由内部进程发起的会话

答案:D

【分析】 入站规则用于禁止输入或允许输入会话发起方发送的用于创建会话的报文。因此,只能用于禁止或允许创建由外部进程发起的会话。

(19) 关于出站规则,以下哪一项描述是错误的?(　　)

A. 可以用 IP 地址唯一指定会话响应方所在的终端

B. 可以用端口号唯一指定作为会话响应方的进程

C. 可以用协议指定会话类型

D. 出站规则用于禁止或允许创建由外部进程发起的会话

答案:D

【分析】 出站规则用于禁止输出或允许输出会话发起方发送的用于创建会话的报文。因此,只能用于禁止或允许创建由内部进程发起的会话。

(20) 关于 ping 命令,以下哪一项描述是错误的?(　　)

A. 发送若干个 ICMP ECHO 请求报文

B. 用序号和标识符匹配 ICMP ECHO 请求和响应报文

C. ICMP ECHO 请求和响应过程成功则表明与目标主机连通

D. ICMP ECHO 请求和响应过程失败则表明不存在与目标主机之间的传输路径

答案:D

【分析】 ICMP ECHO 请求和响应过程失败则表明没有接收到目标主机发送的与 ICMP ECHO 请求报文匹配的 ICMP ECHO 响应报文,发生这一情况的原因很多,不存在与目标主机之间的传输路径只是一种可能的原因,目标主机防火墙禁止发送与 ICMP ECHO 请求报文匹配的 ICMP ECHO 响应报文也是一种可能的原因。

(21) 关于 tracert 命令,以下哪一项描述是错误的?(　　)

A. 不断发送 ICMP ECHO 请求报文,直到接收到匹配的响应报文

B. 依次递增封装 ICMP ECHO 请求报文的 IP 分组的 TTL 字段值

C. 与目标主机之间的传输路径经过的所有路由器依次发送超时报文

D. 封装超时报文的 IP 分组以目标主机的 IP 地址为源 IP 地址

答案:D

【分析】 当封装 ICMP ECHO 请求报文的 IP 分组到达某台路由器时,如果 TTL 值减为 0,则该路由器向源终端发送一个超时报文,超时报文封装成以该路由器接收该 IP 分组的接口的 IP 地址为源 IP 地址、源终端的 IP 地址为目的 IP 地址的 IP 分组。

(22) 一台主机用浏览器无法访问到域名为 www.pku.edu.cn 的服务器,并且在这台主机上执行 ping 命令时有如下信息。

```
C:\>ping www.pku.edu.cn
ping www.pku.edu.cn[162.105.131.113] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 162.105.131.113
Packets: Sent=4,Received=0,Lost=4(100% loss)
```

分析以上信息,可以排除的故障原因是(　　)。

A. 网络链路出现故障

B. 主机浏览器工作不正常

C. 服务器 www.pku.edu.cn 工作不正常

D. 主机设置的 DNS 服务器工作不正常

答案:D

【分析】 由于已经成功完成完全合格的域名至 IP 地址的转换过程,说明 DNS 工作正常。

(23) 一台主机用浏览器无法访问到域名为 www.pku.edu.cn 的网站,并且在这台主机上执行 tracert 命令时有如下信息,可能的原因是(　　)。

```
Tracing route to www.pku.edu.cn[72.5.124.61]
Over maximum of 30 hops
1 <1ms <1ms <1ms   202.113.64.129
2   202.113.64.129 reports:Destination net unreachable
trace complete
```

A. 主机 IP 地址设置有误

B. 相关路由器设置了访问控制

C. 服务器 www.pku.edu.cn 工作不正常

D. 主机设置的 DNS 服务器工作不正常

答案:B

【分析】 错误的原因是 TTL 为 2 的 ICMP ECHO 请求报文无法到达第二跳路由器。

(24) 在一台主机上用浏览器无法访问到域名为 www.online.tj.cn 的网站,并且在这台主机上执行 tracert 命令时有如下信息:

```
Tracing route to www.online.tj.cn [202.99.64.102]
over a maximum of 30 hops:
1     <1 ms    <1 ms    <1 ms     202.113.64.129
2     <1 ms    <1 ms    <1 ms     202.113.77.1
...
16    *        *        *        Request timed out.
17    *        *        *        Request timed out.
```

```
Trace complete.
```

分析以上信息,可能造成这种现象的原因是(　　)。

A. 该计算机的网关地址设置有误

B. 该计算机设置的 DNS 服务器工作不正常

C. 该计算机的 IP 地址与子网掩码设置有误

D. 网站 www.online.tj.cn 工作不正常

答案:D

【分析】 已经接收到第一跳路由器发送给它的 ICMP ECHO 响应消息,因此,该计算机的 IP 地址、子网掩码和网关地址设置正确。由于已经解析出域名 www.online.tj.cn 对应的 IP 地址,因此,域名服务器工作正常,得出可能的原因是网站 www.online.tj.cn 工作不正常。

(25) 在已经获取 IP 地址的 DHCP 客户端上执行命令 ipconfig/release 后,该 DHCP 客户端上的 IP 地址和子网掩码分别是(　　)。

A. 169.254.161.12 和 255.255.0.0

B. 0.0.0.0 和 0.0.0.0

C. 127.0.0.1 和 255.255.255.255

D. 127.0.0.1 和 255.0.0.0

答案:B

【分析】 选择 DHCP 自动获取 IP 地址方式,且未从 DHCP 服务器获取 IP 地址时,IP 地址和子网掩码分别是 0.0.0.0 和 0.0.0.0。

14.3　名词解释

(1) 主体

主动的实体,通常包括用户、进程和服务等。

(2) 客体

包含或接收信息的被动实体,通常包括文件、程序、目录、数据库等。

(3) 访问

使信息在主体和客体间流动的一种交互方式。

(4) 访问控制

一种具有以下两个功能的安全机制,一是能保障授权用户获取所需资源,二是能拒绝非授权用户非法获取资源。

(5) 授权

为每一个用户设置访问权限。

(6) 访问控制策略

主体对客体的访问规则集,这个规则集直接定义了主体对客体的作用行为和客体对主体的条件约束。

(7) 访问控制模型

访问控制策略的形式化和实现机制描述,包含主体、客体和主体对客体的操作。

(8) 自主访问控制(DAC)

基于主体或主体所属的主体组的身份限制主体对客体的访问。

(9) 访问控制矩阵

以矩阵的形式描述一组主体对一组客体的访问权限。

(10) 访问控制表

针对每一个客体,列出所有允许访问该客体的主体和主体对该客体的访问权限。

(11) 访问能力表

针对每一个主体,列出所有允许该主体访问的客体和该主体对客体的访问权限。

(12) 强制访问控制(MAC)

对所有主体及所控制的客体实施强制访问控制。

(13) BLP 模型

一种通过实施不上读/不下写的访问原则,保证数据保密性的强制访问控制模型。

(14) Biba 模型

一种通过实施不下读/不上写的访问原则,保证数据完整性的强制访问控制模型。

(15) 基于角色的访问控制(RBAC)

一种为角色配置访问权限,用户根据承担的角色获取该角色的访问权限的访问控制方式。

(16) 审计

对日志进行分析,并以清晰且能理解的方式表述分析结果。

(17) 入站规则

一系列用于禁止或允许输入会话发起方发送的用于创建会话的报文的规则。

(18) 出站规则

一系列用于禁止或允许输出会话发起方发送的用于创建会话的报文的规则。